NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

MBA PROFESSIONAL REPORT

Commander’s (Executive Officer’s) Guide for Detecting and Deterring Procurement Frauds in Military Unit (Organization) Of Armed Forces of Ukraine

By: Vadym Voloshenko

June 2009

Advisors: Juanita M. Rendon,
Jim Suchan

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2009	**3. REPORT TYPE AND DATES COVERED** MBA Professional Report

4. TITLE AND SUBTITLE Commander’s (Executive officer’s) Guide for Detecting and Deterring Procurement Frauds in Military Unit (Organization) of Armed Forces of Ukraine

5. FUNDING NUMBERS

6. AUTHOR(S) Vadym Voloshenko

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

The objective of this project is to review the best practices of American organizations in the areas of internal control and fraud prevention and to provide guidelines for fraud detection and fraud deterrence for commanders in the Ukrainian Armed Forces. Financial control system in Ukrainian Armed Forces is historically based on professional audit. Decentralization of management and control is a current trend in the military organization. The Cabinet of Minister of Ukraine developed a long-term strategy to establish an internal control system throughout the Ukrainian government including the uniformed services. Conceptually, this system will be based on the U.S. Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework, which de-facto is becoming a global standard. Under current transformational conditions, the suggested project can work as an internal-control outpost and increase general awareness of commanders or top-level managers about internal control effectiveness and fraud prevention.

14. SUBJECT TERMS Internal Control, Fraud Management, Ukraine

15. NUMBER OF PAGES
139

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

COMMANDER'S (EXECUTIVE OFFICER'S) GUIDE FOR DETECTING AND DETERRING PROCUREMENT FRAUDS IN MILITARY UNIT (ORGANIZATION) OF ARMED FORCES OF UKRAINE

Vadym Voloshenko, Colonel, Ministry of Defense of Ukraine

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF BUSINESS ADMINISTRATION

from the

NAVAL POSTGRADUATE SCHOOL
June 2009

Author: ______________________________
Vadym Voloshenko

Approved by: ______________________________
Juanita M. Rendon, Lead Advisor

____
Jim Suchan, Support Advisor

____
William Gates, Dean
Graduate School of Business and Public Policy

THIS PAGE INTENTIONALLY LEFT BLANK

COMMANDER'S (EXECUTIVE OFFICER'S) GUIDE FOR DETECTING AND DETERRING PROCUREMENT FRAUDS IN MILITARY UNIT (ORGANIZATION) OF ARMED FORCES OF UKRAINE

ABSTRACT

The objective of this project is to review the best practices of American organizations in the areas of internal control and fraud prevention and to provide guidelines for fraud detection and fraud deterrence for commanders in the Ukrainian Armed Forces. Financial control system in Ukrainian Armed Forces is historically based on professional audit. Decentralization of management and control is a current trend in the military organization. The Cabinet of Minister of Ukraine developed a long-term strategy to establish an internal control system throughout the Ukrainian government including the uniformed services. Conceptually, this system will be based on the U.S. Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework, which de-facto is becoming a global standard. Under current transformational conditions, the suggested project can work as an internal-control outpost and increase general awareness of commanders or top-level managers about internal control effectiveness and fraud prevention.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Professor Juanita M. Rendon, the first professor who introduced me to the subject and importance of internal control, for her titanic efforts. Without her help and guidance, the completion of this professional report would not have been possible. Under time pressure circumstances she dedicated not just high-quality expert knowledge, but also inspired and encouraged me personally.

I would like to thank Professor Jim Suchan for his high-quality expert input and endless patience.

I would also like to thank my family for their support and understanding.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. CHAPTER OVERVIEW

The objective of this project is to review the best practices of American organizations in the areas of internal control and fraud prevention and to provide guidelines for fraud detection and fraud deterrence for commanders in the Ukrainian Armed Forces. This chapter covers the background, purpose of this project, research objectives and methodology, definitions, and organization of this report.

B. BACKGROUND

1. Challenges that Increase the Risk of Fraud in the Ukrainian Armed Forces

Although internal control concepts and regulations are used against fraud in modern practice, leaders and managers of the Ukrainian Armed Forces face several challenges that increase the risk of fraudulent activity.

a. Decentralization of Management

Historically, the Ukrainian Armed Forces combined an inherited highly centralized system of military control with a decentralized system of economic management for the same entity—the military unit.

On one hand, the military chain of command customarily assumes that directives from a central command will be followed rigorously without deviation. Sometimes this rigidity introduces absurd situations, such as when a unit's commander cannot make decisions in his area of responsibility without special approval from someone in the upper ranks. He becomes indecisive and is undermined as a leader. In addition, granting approval demands a lot of time and energy from higher command, so the efficiency of the process suffers greatly.

On the other hand, since World War II, every military unit in Ukraine has its own materiel base. A typical organization (or unit) is accountable for its own buildings, depots, and other permanent assets. Every unit has its own supply system (actually a mix of centralized supply and local purchasing from domestic producers) and separate accounts for all supply categories, from food and gas to armaments. A military unit not only has its own budget, but also its own banking accounts, and pays for all its expenses. Thus, a Ukrainian unit is a self-sufficient organization comparable in its economic functions to a business.

The military effectiveness of this centralized/decentralized structure may be questioned because of its lack of flexibility and the large number of noncombatant military personnel performing managerial functions. To improve the economic management of the military unit, managerial control offers significant advantages. A commander can have the authority to make his managerial decisions in response to the local environment, resulting in more flexibility and less time wasted waiting for directives from a central authority. The quality of local managerial decisions depends heavily on the knowledge and moral character of the commander.

The Ukrainian Armed Forces' current system of control cannot be equally effective for highly centralized military relations and for decentralized economic relations inside the unit. Military units need more guidance which can be transformed into an internal commander's decisions, rather than Ministry directives.

b. Complexity of Environment

Complexity negatively impacts accountability and transparency. Today's Ukrainian military operates in an environment of unprecedented complexity. Ukraine is creating a new, interoperable armed forces by transforming the old Soviet-era military organization. Such transformational periods create extra complexity. For example, there are currently two simultaneous accounting systems for financial management, one based on old regulations and the other based on modern principles. Theoretically, a dual accounting system should insure the whole financial structure against glitches in the new accounting system, which needs testing and tuning before being incorporated. However, maintaining two separate accounting systems has created unintended consequences. The internal and external consumers of accounting information rely on different sets of unconnected books, thus creating an opportunity for intentional misrepresentation of factual transactions in either of the systems while also doubling the auditor's scope of work.

C. PURPOSE OF THIS PROJECT

The military management (control) is a distinctive realm, far different from the civilian business world. The knowledge behind effective command of the battlefield has nothing in common with economics. These fields of expertise are as far removed as destruction from creation.

Effective leadership has a different meaning than management. The typical officer can inspire and motivate people for combat, but has a weak knowledge of accounting, contracting, and supply management, and needs assistance to fight financial fraud. Director of Financial Department of Ministry of Defense of Ukraine Ivan Marko claimed that a poor understanding of financial principles and the lack of control within the military units are the biggest source of fraud in the Ukrainian ministry of defense. (Outlines of director's speech, 2008).

In May 2008, the director of finances for the Ukrainian Ministry Of Defense stated that total losses from fraudulent activity in 2006–2007 had climbed to $600,000[1] . Seventy-eight percent of that total involved cash-related frauds, and other fraudulent activities totaling $200,000[2] were not discovered by external auditors for several years (Outlines of director's speech, 2008). The greatest area of concern was fraud that involved the financial comptrollers of military units and stemmed from both a lack of internal controls and irresponsible practices among commander executives. The absence of internal control in military units or organizations often stems from the lack of clear, concrete guidance on how to establish controls.

Providing commanders with practical guidance, as this project attempts to do, should not only assist in the understanding of internal controls and fraud prevention but also provide reliable tools for fraud detection and fraud-risk assessment, based on the experience of American organizations that are fighting fraud.

D. RESEARCH OBJECTIVES AND METHODOLOGY

This project is focused on the following research objectives:

- To identify individual, organizational, and societal factors that can cause a fraud;
- To organize the factors into early-warning systems that can be used to detect and deter fraud.
- To develop a guide to assist military commanders in detecting and deterring fraud.

This project is applied research[3]. The main method for this research is deductive reasoning from extensive review of fraud-related literature.

E. DEFINITIONS

1. Fraud and Internal Control Defined

Fraud has been an ongoing issue for thousands of years and continues to be a problem today. There are several definitions for fraud as a legal (or criminal) concept. According to the Encyclopedia Britannica, fraud is “the deliberate misrepresentation of fact for the purpose of depriving someone of a valuable possession. Although fraud is sometimes a crime in itself, more often it is an element of crimes such as obtaining money by false pretense or by impersonation” (Britannica, 2009). To understand the components of fraud, a systematic approach is in order. As a system, fraud involves victims and perpetrators, and as a structure, it involves a fraud scheme. Fraud can be evaluated as an open system[4], and the challenge is to evaluate the weaknesses of this system in order to impact it (detect, prevent, or deter). One of the most effective systems for deterring fraud is internal control.

Internal control is a system by definition, operating in the same environment as the fraud itself and serving as an effective, formidable adversary to the fraud scheme. The usual definitions of internal control, described as a process, framework, or function, do not touch upon systematic concepts (as discussed in Chapter II). The most widely used definition is that of the Committee of Sponsoring Organizations of the Treadway Commission (COSO):

> a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> Effectiveness and efficiency of operations.
>
> Reliability of financial reporting.
>
> Compliance with applicable laws and regulations.
>
> (Internal Control —Integrated Framework, 1992, p.13).

F. ORGANIZATION OF THIS REPORT

This MBA project is composed of six chapters. Chapter I discusses the background, purpose of this project, research objectives and methodology, definitions, and organization of the report. Chapter II contains a literature review and describes modern fraud management and internal control practices, summarizing United States anti-fraud regulations and the experience of American corporations in combating fraud. Chapter II also describes the author's vision of the application of the COSO internal control framework to military organizations and uncovers challenges in managing procurement fraud. Chapter III focuses on the control system of the Ukrainian Ministry of Defense, which is based on the effective audit network that oversees the financial activity of organizations. Chapter IV analyses the importance of changing leadership styles to inspire transformational changes in Ukrainian Armed Forces. In addition, this chapter shows the benefits of implementing a fraud-management system at the organizational level. Chapter V will provide a sample guide, which, upon approval by the Ukrainian

Ministry of Defense, can be distributed to military commanders for practical application. Finally, Chapter VI summarizes the project, draws conclusions, and recommends improvements.

The next chapter will provide a literature review on internal control and fraud management.

II. LITERATURE REVIEW

A. INTRODUCTION

The concept of internal control has developed over time within the United States federal government and American corporations. This chapter provides a theoretical basis on which to establish solutions for practical internal control problems. A review of the literature reveals three major observations concerning successful American models.

First, over the last decades, federal agencies have been the subject of significant internal control discussions and legislation. The “Office of Management and Budget Circular A-123 of 1981,” the “Federal Managers’ Financial Integrity Act of 1982” (FMFIA), the GAO’s *Standards for Internal Control in the Federal Government*, and DoD directives 5010.38 and 5010.40 serve as consistent guidelines.

Second, the modern governmental approach to internal control closely parallels developments in the private sector. Private-sector regulations in the twentieth century were poorly developed; however, the Sarbanes-Oxley Act of 2002 created a general framework to reduce that deficiency for the biggest market players - publicly traded companies. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), formed in 1985, is a voluntary private-sector organization devoted to providing guidance for establishing effective, efficient, and ethical business practices globally. The COSO *Internal Control—Integrated Framework* (COSO ICIF) became the bible of internal control and was adopted by government agencies in later revisions of OMB Circular A-123, GAO *Standards for Internal Control in the Federal Government*, as well as the Public Company Accounting Oversight Board Auditing Standard Nos. 2 and 5.

Third, criminological approaches to fraud allow for a new understanding and for new perspectives on fraudulent activities and the relationship to internal control. The American Institute of Certified Public Accountants (AICPA) issued Statement on Auditing Standards [SAS] No. 99, *Consideration of Fraud in a Financial Statement Audit* which puts into practice standards for all auditors related to detecting fraud. Several risk factors recognized as related to fraudulent activities are adopted from criminological theories.

This chapter will discuss internal control basics and several federal legislation that has taken place over the years related to internal control, In addition, the COSO Internal Control framework and fraud management will be reviewed.

B. INTERNAL CONTROL 101

Internal controls for accounting involve a system of checks and balances to prevent loss of any kind, whether due to fraud, waste, poor supervision, or errors. Organizations historically define internal control differently depending on their objectives. O. Ray Whittington and Kurt Pany, professors and CPAs, observe that meaning and objectives of internal control are still changing. If in the 1990's, people were concerned about fraud prevention as a primary internal control objective, now more people believe that internal control is equally important for fraud deterrence and for assuring control over operations and other processes.(Whittington & Pany, 2008)

One of the first official definitions of internal control given by the American Institute of Accountants in 1949 is as follows:

> Internal control comprises the plan of organizing and all of the co-ordinate methods and measures adopted within a business to safeguard its assets, check the accuracy and reliability of its accounting data, promote operational efficiency, and encourage adherence to prescribed managerial policies" (Cadmus, 1953, p. 4)

A detailed definition of internal control was expressed by the AICPA Auditing Standards Board in SAS No. 112 in 2006:

> Internal control is a process—effected by those charged with governance, management, and other personnel—designed to provide reasonable assurance about the achievement of the entity's objectives with regard to reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations. Internal control over the safeguarding of assets against unauthorized acquisition, use, or disposition may include controls related to financial reporting and operations objectives. Generally, controls that are relevant to an audit of financial statements are those that pertain to the entity's objective of reliable financial reporting. In this section, the term financial reporting relates to the preparation of reliable financial statements that are fairly presented in conformity with generally accepted accounting principles. The design and formality of an entity's internal control will vary

> depending on the entity's size, the industry in which it operates its culture, and management's philosophy. (AU Section 325, 325.03)

There are other definitions and models as well. For example, the *Encyclopedia of Business and Finance* suggests several modern internal control models. The Canadian Institute of Chartered Accountants in *Guidance on Control* offers the model named Criteria of Control (CoCo). CoCo describes internal control as actions focused on

- effectiveness and efficiency of operations
- reliability of internal and external reporting
- compliance with applicable laws and regulations and internal policies

The CoCo model combines four elements of internal control:

- purpose (the objective to be achieved by the task)
- capability (information, resources, supplies, and skills)
- commitment
- monitoring and learning (monitoring task performance to improve the process)

The Institute of Internal Auditors Research Foundation issued *Systems Auditability and Control* (SAC) which defines internal control as "a set of processes, functions, activities, subsystems, and people who are grouped together or consciously segregated to ensure the effective achievement of objective and goals" (that is, of internal control systems) (Internal Control Systems, 2009, p.2).

All these definitions address objectives for internal control, processes, and the variables that influence processes (functions, subsystems, etc.). The most comprehensive definition can be found in the COSO ICIF, which will be discussed in detail and serve as a basis for developing a practical internal control guide for military commanders.

The primary objectives of internal control are fraud management and improving the effectiveness and efficiency of operations. All other objectives are combinations or derivatives of these. For example, the objective of complying with laws and regulations has fraud prevention or efficiency as its ultimate object. This project focuses on fraud prevention alone and does not discuss other considerations.

The next section contains a brief history of official attempts to exercise internal control and traces how theories have been incorporated into procedures. Some early documents have purposely been omitted because they are insignificant to modern anti-fraud measures.

C. FEDERAL LEGISLATION

The executive branch of the United States oversees the effectiveness and efficiency of federal agencies, and as a result, has substantial regulation of these agencies.

1. OMB Circular A-123

The Presidential Office of Management and Budget (OMB) in October, 1981 released Circular A-123,[5] "Internal Control Systems." This circular categorized internal control issues for federal agencies, establishing standards in anticipation of FMFIA's[6] becoming law. In December 1982, following FMFIA enactment, the OMB issued the assessment guidelines as required by the act. The OMB's *Guidelines for the Evaluations and Improvement of and Reporting on Internal Control Systems in the Federal Government* detailed a seven-step assessment targeted towards an agency's mission and organizational structure. The comptroller general subsequently issued *Standards for Internal Control in the Federal Government*[7] in 1983 (United States Congress, House Hearing, 2005).

In December of 2004, OMB published the most recent revision of Circular A-123, updated for the reason of better compliance with the standards under Sarbanes-Oxley. Congressman Todd Russell Platts, chairman of the Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform, observed that revised guidance increases responsibility of governmental agencies' management and better defines the necessary actions that need to be done to ensure effectiveness of internal controls (United States Congress, House Hearing, 2005).

In testimony before the House Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform, Jeffrey C. Steinhoff, managing director of financial management and assurance for the GAO, stated that the updated version of circular A-123 correctly framed internal control systems not merely as an isolated management tool but as an integral part of the cycle of planning, budgeting, management, accounting, and auditing. (United States Congress, House Hearing, 2005).

The most significant features of revised OMB Circular A-123 are found in the Table 1.

Content	Section
1. Fostered compliance with the Sarbanes-Oxley Act (Appendix A, Chapter I)	The passage of the Sarbanes-Oxley Act served as an "impetus for the federal government to reevaluate its current policies relating to internal control over financial reporting and management's related responsibilities" (OMB Circular A-123, 2004, p.20).
2. Adopted COSO framework (Chapter II)	The objectives of internal control are: • effectiveness and efficiency of operations, • reliability of financial reporting • compliance with applicable laws and regulations. "Management is responsible for developing and maintaining internal control activities that comply with the following standards to meet the above objectives: • control environment • risk assessment • control activities • information and communications monitoring" (OMB Circular A-123, 2004, p.7).
3. Based definitions of control deficiency, reportable condition, and material weakness relative to financial reporting upon the definitions provided in "Auditing Standard No. 2" issued by the Public Company Accounting Oversight Board	"A *control deficiency* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A *design deficiency* exists when a control necessary to meet the control objective is missing or an existing control is not properly designed, so that even if the control operates as designed the control objective is not

(PCAOB). (Appendix A, Chapter II, D)	always met. An *operation deficiency* exists when a properly designed control does not operate as designed or when the person performing the control is not qualified or properly skilled to perform the control effectively.” (OMB Circular A-123, 2004, p.23).
4. Defined algorithm for assessing internal control system:	
Proper usage of sources of information (Chapter IV, A)	“Management has primary responsibility for assessing and monitoring controls, and should use other sources as a supplement to—not a replacement for—its own judgment” (OMB Circular A-123, 2004, p.13).
Identification of deficiencies (Chapter IV, B)	“Agency managers and employees should identify deficiencies in internal control from the sources of information described above and the results of their assessment process” (OMB Circular A-123, 2004, p.14).
Reporting on internal control (Chapter VI, A)	“Assurance statement should include the annual assurance statements, summary of material weaknesses and non-conformances, and summary of corrective action plans.” (OMB Circular A-123, 2004, p.17).
Correcting internal control deficiencies (Chapter V)	“Agency managers are responsible for taking timely and effective action to correct deficiencies identified by the variety of sources” (OMB Circular A-123, 2004, p.15).

Table 1. Features of OMB Circular A-123 in revision December 2004

In summary, OMB Circular A-123 is the most substantial governmental document regulating internal control issues. Because it adopts the broadest perspectives, concepts, and procedures from legislation and corporate regulation, OMB Circular A-123 will be used as the primary source for a practical guide for military commanders for detecting and deterring procurement fraud in Ukrainian military units.

2. The Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act of 2002 (SOX) was enacted in response to accounting scandals in the late 1990s and early 2000s to revive investment activity and ensure soundness of financial reports of publicly traded corporations. Enacted on July 30, 2002, SOX focuses on improving quality, reliability, and transparency in financial reporting, independent audits, and accounting services for all companies regulated by the Securities and Exchange Commission (SEC).

By this act, Congress required that:

> Each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m or 78o(d)) to contain an internal control report, which shall—(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting. (Sarbanes-Oxley Act of 2002, sec 404a)

> With respect to the internal control assessment required by subsection (a), each registered public-accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. (Sarbanes-Oxley Act of 2002, sec 404b)

The Sarbanes-Oxley Act contains eleven titles with specific requirements for financial reporting that establish various deadlines for compliance, reporting requirements, and standards for integrating auditing and accounting. The Act also established the Public Company Accounting Oversight Board (PCAOB) to oversee the accounting profession. This five-member board, under the authority of the SEC, has the responsibility of establishing or adopting auditing, attestation, quality control, ethics, and independence standards in the preparation of audit reports for SEC registrants, which are publicly-traded companies in the United States. (Whittington & Pany, 2008)

3. DoD Directive 5010.38; Management Control Program

In August 26, 1996, the Department of Defense (DoD) issued a current update of Directive 5010.38, the *Management Control (MC) program*, to establish policy and assign responsibilities (DoD 5010.38, 1996) for implementing the requirements of OMB Circular A-123. The current directive applies throughout the DoD, including the Office of the Secretary of Defense (OSD), military departments, and defense agencies including field activities, which are collectively referred to as DoD components (DoD 5010.38, 1996, p.1).

Current policy, under DoD directive 5010.38, mandates that each DoD component design and implement comprehensive strategies for internal controls that provide reasonable assurance in several areas. Specifically, this policy requires:

- integration of the MC program into daily practices
- prevention of waste, fraud, and mismanagement, as well as timely correction of MC weaknesses
- continual monitoring and improvement of MC effectiveness
- reliance on different sources of information
- management involvement at all levels
- assigning and training of MC managers (focusing on obligations and responsibilities)

In addition, this directive assigns general responsibility to top DoD management, the Office of the Under Secretary of Defense (Comptroller). In summary, Directive 5010.38 establishes a framework and direction for in-depth development of MC programs.

4. DoD Instruction 5010.40: Managers' Internal Control Program Procedures

The DoD issued Instruction 5010.40, *Management Control [MC] Program Procedures,* on August 28, 1996. On January 4, 2006, the directive was updated (at the same time as the instruction of 1996 was canceled) and the name changed to *Managers' Internal Control [MIC] Program Procedures*.

DoD Instruction 5010.40 emphasizes the Federal Manager's Financial Integrity Act (FMFIA), as implemented through the DoD Managers' Internal-Control Program, that requires all DoD managers “to review, assess, and report on the effectiveness of internal controls (ICs) within the Department of Defense” (DoD 5010.40, 2006). In addition, the instruction requires that the head of each DoD component assigns direct IC responsibility to civilian and military leaders and provides trained personnel for planning, directing, and implementing the MIC program (DoD 5010.40, 2006).

This instruction cites twenty-three references designed to implement Federal Managers’ Financial Integrity Act and OMB Circular A-123 changes. Generally, Instruction 5010.40 is the DoD adaptation of the last version of OMB Circular A-123 and contains most of the regulations found in the OMB circular. This instruction is useful for the present project because its concise organization and style tend to be user-friendly to military persons, providing easy reference to exact points and issues.

For example, OMB Circular A-123 describes management’s process for resolution and corrective action in general, vague terms such as “assure that performance appraisals of appropriate officials reflect effectiveness in resolving or implementing corrective action for identified material weaknesses.” DoD Instruction 5010.40 for the same action defines a six-point procedure that contains clear, specific statements such as “require corrective action plans that show progress on a quarterly basis at a minimum,” or “the last milestone in each corrective action plan shall include a correction validation unless a metric is used, in which case, the final corrective action shall describe how the metric goal was met.” A shortcoming of this document, however, is that it assumes the military manager has already received thorough training and has background knowledge in implementing of financial control elements.

To summarize, the purpose of DoD Instruction 5010.40 is to implement the Federal Managers' Financial Integrity Act and OMB Circular A-123 changes. It contains concepts from the most significant sources, including the Sarbanes-Oxley Act of 2002, that increase management’s responsibility over internal control, and from the COSO ICIF.

D. THE COSO INTERNAL CONTROL FRAMEWORK

1. History

The COSO ICIF was prepared in response to recommendations by the National Commission on Fraudulent Financial Reporting. The commission, commonly referred to as the Treadway Commission, was a private-sector initiative jointly sponsored by five professional organizations: American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Institute of Internal Auditors (IIA), Institute of Management Accountants (IMA), and Financial Executives Institute (FEI).

In 1987, the commission recommended that the sponsoring organizations develop additional integrated guidance on internal control. The COSO was formed to support the implementation of the Treadway Commission's recommendations and published the completed ICIF in 1993. (Karl Nagel & Company, LLCs Sarbanes-Oxley, 2009).

2. Definitions

Precise definitions are probably the most significant achievement of the COSO ICIF.

The first main definition is for internal control:

> Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
>
> - Effectiveness and efficiency of operations.
> - Reliability of financial reporting.
> - Compliance with applicable laws and regulations.
>
> (COSO ICIF, 1994, p.13)

This definition enables different approaches for the development of any kind of internal control system. The following elements are defined broadly:

Process: An internal control system is dynamic and cannot be treated as a one-time event or circumstance.

People: Internal control is the effect of people's decisions and actions, which in turn affect other people. People's understanding, communication, and performance are key issues in system functionality. It is a central element of the system.

Objectives: All control objectives fall into three categories: effectiveness and efficiency of operations, reliability of financial reporting, and compliance with laws and regulations. These categories are distinct but overlapping. A particular objective can belong to more than one category; for example, fraud prevention involves all three. The strategies an entity employs may approach objectives discretely or address them all simultaneously.

Limitation of activity: Internal controls can provide only reasonable assurance, not absolute assurance, and, therefore, need to be combined with other types of control. This inherent limitation stems from the inevitability of errors, mistakes, miscommunication, and the possibility of overriding system rules.

The second main definition is of the components of internal control. Internal control consists of five interrelated components. These are derived from the way management runs a business and are integrated with the management process. The components are defined as:

- Control environment: The core of any business is its people—their individual attributes, including integrity, ethical values and competence—and the environment in which they operate. They are the engine that drives the entity and the foundation on which everything rests.
- Risk assessment: The entity must be aware of and deal with the risks it faces. It must set objectives, integrated with the sales, production, marketing, financial and other activities so that the organization is operating in concert. It also must establish mechanisms to identify, analyze and manage the related risks.
- Control activities: Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity's objectives are effectively carried out.

- Information and communication: Surrounding these activities are information and communication systems. These enable the entity's people to capture and exchange the information needed to conduct, manage, and control its operations.
- Monitoring; The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant. (COSO ICIF, 1994, p.16)

The COSO components of internal control can be used as bricks for building any kind of internal control system by augmenting or cutting functions and processes. The following section will discuss these components in more detail.

3. Internal Control Components

The COSO model is depicted as a pyramid, with the control environment providing a base for risk assessment, control activities, and monitoring. Information and communication link the different levels of the pyramid.

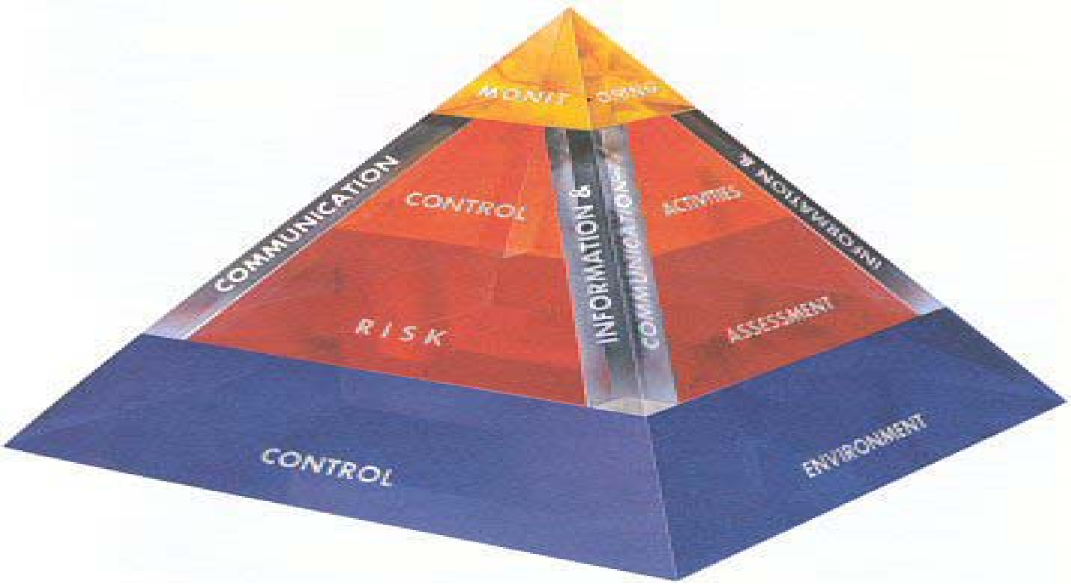


Figure 1. Internal Control Components from COSO ICIF, 1994

a. Control Environment

As the base of the pyramid, the control environment sets the tone for the organization. Factors of the control environment include “the integrity, ethical values, and competence of the entity’s people; management’s philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by the board of directors” (COSO ICIF, 1994, p. 23). The control environment provides discipline and structure for the whole system.

The control environment should reflect several factors. First, the organization should display strong ethical values. This is difficult because various parties have different concerns, incentives, and temptations. Next, all parties should be competent in the performance of their duties. Another important factor that significantly affects the control environment is management’s philosophy and operating style. Furthermore, human-resource policy, including proper assignment of authority and responsibility, adequate training, and promotion and compensation guidelines, greatly influences the control environment. Finally, the appropriate organizational structure enhances the control environment. An organizational structure that is inappropriate for the organization’s tasks that causes bottlenecks in information flow, and results in unclear assignment of responsibility prevent the accomplishment of organizational objectives. (COSO ICIF, 1994)

b. Risk Assessment

Risk assessment denotes the identification, analysis, and management of uncertainties facing an organization from external and internal sources. Risk assessment is highly relevant to control objectives. Because internal control is a dynamic system (economic and operating conditions are continuously changing), mechanisms of risk assessment are also subject to changes and adjustments. Proper setting of objectives is a necessary precondition to effective risk assessment.

Risk assessment looks at both internal and external threats. Rapid growth, changes in personnel or operational processes, new information systems, legislation, or technology, and competition all require adequate control measures. Other considerations outlined in the COSO report include the techniques used in identifying risk such as forecasting, planning, deriving results from internal and external auditor experience, economic reviews, and quantitative and qualitative prioritization. In addition, assessment includes analyzing risks, estimating the significance of a risk and the possibility of it occurring, and considering what action to take in response. Finally, mechanisms used in assessing risk should be flexible and fit the dynamic environment. (COSO ICIF, 1994)

c. Control Activities

Control activities include the policies and procedures maintained by an organization to ensure management directives are carried out. They include a range of activities such as "approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets, and segregation of duties" (COSO ICIF, p. 49). Control activities are the most visible element of internal control and arguably the most important in preventing wrong actions from occurring. However, the COSO suggests that the control environment is more critical because it influences motivation for proper behavior.

Control activities can be easily established and should be considered startup elements for developing the internal control system of a new organization. The COSO identifies six categories of control activities. These categories include segregation of duties, physical controls over cash and other assets, top-level reviews of performance, effective direct management of activities, information processing of transactions, restriction of access to data, investigation of unusual performance indicators, and maintenance of proper documentation of transactions. In addition, the COSO dedicates an entire section to categories specifically related to control activities for information systems, such as data centers, system-software acquisition and maintenance, and access security.

d. Information and Communication

Information and communication concerns include the identification, capture, and exchange of financial, operational, and compliance-related data in a timely manner. People within an organization who have timely, reliable, and understandable information are better able to conduct, manage, and control operations.

Information and communication stress the quality of information. Information should be appropriate, timely, current, accurate, and accessible. All these elements are extremely important and must be applied by the internal control system design; otherwise, the components of the internal control system will be unable to operate as a whole. Information is identified, captured, processed, and reported by information systems.

Information systems can be formal or informal, can operate in routine-monitoring mode or on call, and can be integral part of every activity, whether strategic planning, operations, or control.

The COSO stated that communication is inherent to information systems[8] and can be internal or external.

> Effective communication also must occur in a broader sense, flowing down, across and up the organization. All personnel… must understand their own role in the internal control system, as well as how individual activities relate to the work of others. …There also needs to be effective communication with external parties, such as customers, suppliers, regulators and shareholders. (COSO ICIF, p.59)

The COSO also suggests several practical means for effective communications, which include policy manuals, memoranda, bulletin-board notices, videotaped messages, and the most powerful form of communication, action by management in dealing with subordinates.

e. Monitoring

Monitoring refers to the assessment of the quality of internal control. Monitoring activities provide information about potential and actual breakdowns in a control system. Monitoring can occur through self-assessments, external audits, or through direct testing of a control. It is important that any significant deficiencies be reported to the individual responsible for the activity as well as to management one level higher.

Monitoring can be done in two ways: through ongoing activities or separate evaluations (COSO ICIF, 1994). Ongoing monitoring is performed routinely and includes activities which managers perform routinely like comparisons or reconciliations (COSO ICIF). In fact, ongoing monitoring creates an effective balancing feedback loop for managers' decisions about internal control.

Separate evaluations may vary in scope and frequency which are driven by risks. The more significant risks are the more important are control activities which reduce the risks (COSO ICIF).

E. FRAUD MANAGEMENT

Why present fraud management separately from internal control? The answer lies in approaching fraud as a system that has its own objectives, processes, communication subsystem, and main-elements – perpetrators. From the internal control perspective, fraud is a failure of the system. Thus, if fraud prevention can be an objective of effective internal control, its detection is a separate activity best explained by sociological or criminological approaches.

1. Fraud 101

The 2008 "Report to the Nation" issued by the Association of Certified Fraud Examiners (ACFE) indicated that the typical American organization loses seven percent of its annual revenue to fraud. Applied to the gross domestic annual product for 2008, that equals approximately $994 billion in total losses (ACFE, 2008).

Although it is common knowledge that people and corporations commit fraud, what is seldom understood is why they do it. Understanding the motive behind fraud is important in preventing it.

There are many definitions of fraud and they are difficult to combine into one discrete concept because fraud is multidimensional. Several disciplines, such as psychology, sociology, criminology, and business, have described fraud from their own perspectives, emphasizing different aspects of the problem. For example, one modern fraud definition, suggested by Sridhar Ramamoorti, Certified Public Accountant (CPA), Certified Internal Auditor (CIA), Certified Fraud Examiner (CFE), Certified Financial Services Auditor (CFSA), Certified Risk Professional (CRP), Certified Government Auditing Professional (CGAP), and Certified Government Financial Manager (CGFM), states:

> Fraud involves intentional acts and is perpetrated by human beings using deception, trickery, and cunning that can be broadly classified as comprising two types of misrepresentation: *suggestio falsi* (suggestion of falsehood) or *suppressio veri* (suppression of truth). (Ramamoorti, 2008 p.1)

This definition contains elements from business, sociology, and psychology.

Albrecht, Romney, Cherrington, Payne, and Roe (1982) have examined the problem of detecting and preventing business fraud. Two accounting professors, a professor of organizational behavior, a professor of psychology, and a prison psychologist, respectively, suggest various explanations of the nature of fraud. The most significant, from their perspectives, are psychological and sociological explanations.

2. Psychological Explanation of Fraud

Historically, psychologists have developed two major theories of crime: the psychoanalytic and the learning theory. The most popular psychoanalytic theory states that fraud perpetrators are “sick.” According to Sigmund Freud, such sickness can be caused by malfunctions in the individual’s development. Fraud can have its origins in a person's *id*, that part of the personality that seeks to satisfying needs and desires. Under this model, the perpetrator fails to control the impulses of the id. Another malfunction contributing to fraud is found in the action of the underdeveloped conscience, or *superego*. This theory suggests that fraud stems from lack of parental identification and social training. Since the patient's dishonesty does not create feelings of guilt, he may commit fraud whenever there is an opportunity (Albrecht et al., 1982).

A second psychological explanation of fraud derives from the learning theory, which suggests that fraudulent behavior is determined by environmental factors. Individuals will do what their environment teaches them to do. If a person is reinforced for honesty, he or she will be honest; if for dishonesty, the person will be dishonest. Most fraudulent behavior is learned by "operant conditioning, where behavior is influenced by the kinds of rewards and punishments that are associated with it" (Albrecht et al., 1982, p.32). For example, successfully obtaining extra income or removal of impending debts by fraud reinforces fraudulent behavior. Under this theory, "perpetrators become involved in crime after being reinforced for some small, illegal act that encourages them to do more" (Albrecht et al., 1982, p.32). By this theory, indirect experience is very important. Potential perpetrators see others rewarded for successful crimes, increasing the probability that they will act in similar behaviors.

3. Sociological Explanations of Fraud

Sociological explanations of fraud are quite similar to the learning theory. Albrecht et al., 1982 discusses two of the best-known explanations, Sutherland's "differential association" theory and Cressey's "nonshareable need" theory. Both theories go deeper than learning theory in explaining the motivations of perpetrators.

In Sutherland's view, criminal behavior is linked to a criminal environment. The primary source for criminal learning is social interactions with individuals having criminal tendencies.

Albrecht et al., 1982 summarized major elements of differential-association theory as follows:

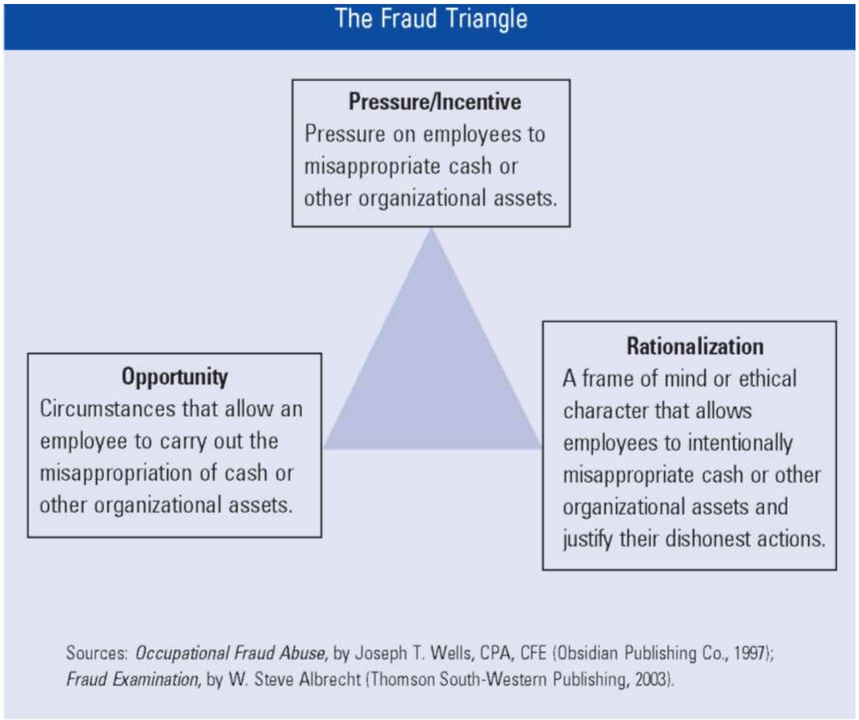
> Criminal behavior is learned; it is not inherited, and the person who is not already trained in crime does not invent criminal behavior. Criminal behavior is learned through interaction with other people, through the processes of verbal communication and example. The principle learning of criminal behavior occurs with intimate personal groups. The learning of crime includes learning the techniques of committing the crime, and the

> motives, drives, rationalizations, and attitudes that accompany it. A person becomes delinquent because of an excess of definitions (or personal reactions) favorable to the violation of the law over definitions unfavorable to the violation of the law. (Albrecht et al, 1982, p.34)

Another sociological theory of fraud was suggested by Dr. Donald Cressey, a notable teacher and pioneer in fraud research who developed the fraud triangle theory. Albrecht et al., 1982 describe the main concepts of Cressey's "nonshareable need" theory. Fraud is a "violation of a position of financial trust" that a person originally took in good faith. Trusted persons become trust violators only if the following three elements occur: "(1) a nonsharable problem, (2) an opportunity for trust violation, and (3) a set of rationalizations that define the behavior as appropriate in a given situation. None of these elements alone would be sufficient to result in embezzlement" (Albrecht et al., 1982, p.34).

4. Fraud Triangle

An important conceptual framework in understanding fraud is the "fraud triangle, which is derived from Cressey's theory, widely disseminated by the Association of Certified Fraud Examiners, and mirrored in AICPA's SAS No. 99. The fraud triangle has three elements, which include perceived incentives and pressures, perceived opportunities, and rationalization of fraudulent behavior (see Figure 2). All three elements of the fraud triangle reciprocally influence the fraud perpetrators' psychology and philosophy.


The Fraud Triangle
Pressure/Incentive
Pressure on employees to misappropriate cash or other organizational assets.
Opportunity
Circumstances that allow an employee to carry out the misappropriation of cash or other organizational assets.
Rationalization
A frame of mind or ethical character that allows employees to intentionally misappropriate cash or other organizational assets and justify their dishonest actions.

Sources: *Occupational Fraud Abuse*, by Joseph T. Wells, CPA, CFE (Obsidian Publishing Co., 1997); *Fraud Examination*, by W. Steve Albrecht (Thomson South-Western Publishing, 2003).

Figure 2. The Fraud Triangle

a. Incentives/Pressures/Motivation

There are many motivations for fraud, most related to greed (as a character stated in the movie “Wall Street,” “greed is good”). Albrecht et al. (1982) identifies at least twenty-five different motivations, including living beyond one’s means, immediate financial need, debts, poor credit, a drug or gambling addiction, and family pressure. Sometimes a perpetrator commits fraud to help his company improve financial results.

In addition, Albrecht et al., 1982 discusses emotional (personal psychological) motives. Beside greed, sometimes pride (“catch me if you can”), impatience, or power play a role. An employee may feel anger and hostility against a company or have a “revenge motive” to make the organization pay for perceived inequities. Pressure to perform is often a motive for fraud.

b. Opportunity

Albrecht et al., 1982 states that opportunities to commit fraud should be assessed from two perspectives:

- opportunities that individuals create for themselves (for example, increasing their knowledge about an organization's operations, advancing to a position of trust, or being the only person who knows a sensitive procedure such as modifying computer programs)
- opportunities created by an organization's poor internal control system (opportunity increases under complex business structures, liberal accounting practices, or high management turnover)

Out of the three fraud triangle elements, opportunity is the one where fraud prevention can excel. In fact, opportunities for fraud are the same elements that occur as deficiencies of internal control system. Effective internal control is absolutely critical to deter opportunity in a fraud prevention program.

c. Rationalization/Integrity

The third element of the fraud triangle is rationalization. Personal integrity and personal code of ethics are key to this fraud element.

Most researchers, such as W. Steve Albrecht, Chad Albrecht, Conan C. Albrecht , and Sridhar Ramammoorti agree that rationalization is a more complex issue than mere determination as to whether a person is honest or dishonest. For example, Albrecht et al., 2008 refer to modern social decoys, or "role models"—politicians, athletes, and movie stars—who are no longer examples of honesty and integrity. Moreover, Albrecht et al., 2008 qualify educational failure as a fraud-reasoning factor because a large majority of students do not understand ethical dilemmas and "would not recognize a fraud if it hit them between the eyes" (Albrecht et al., 2008, p.5). In addition, Peter Goldmann 2008, editor and publisher of the monthly newsletter, "White-Collar

Crime Fighter" suggests a new, extra rationalization factor: the present mass layoffs inducing a feeling of insecurity, isolation, and hopelessness, and erosion of healthcare and pension benefits.

d. The American Dream Theory of Fraud

An interesting development in the fraud triangle theory is suggested by Freddie Choo and Kim Tan of San Francisco State University, 2006. The term "the American dream" was introduced into contemporary social analysis in 1931 by historian James Truslow Adams to describe his vision of a society open to individual achievement (Choo and Tan, 2006).

An American-dream theory of crime in the United States was introduced in 1994 by Stephen F. Messner and Richard Rosenfeld, contemporary criminologists in their work, "Crime and the American Dream." The basic idea of the American-dream theory is that "the pursuit of monetary success (i.e., the institution of economy) has come to dominate the American society, and that the non-economic institutions (i.e., the institution of education, the institution of polity, and the institution of family) have tended to become subservient to the economy" (Choo and Tan, 2006, p.208). This theory has become an effective complement to the fraud triangle theory. Application of the American-dream theory revolves around three key points including "Intense emphasis on monetary success, corporate executives exploiting/disregarding regulatory controls, and corporate executives justifying/rationalizing fraudulent behavior, which have their institutional underpinnings in the capitalist economy of the United States" (Choo and Tan, 2006, p.211)..

The American society is not uniquely materialistic; the same strong interest in material well being is found in most European societies. Modern Ukrainian society, for example, shares a preoccupation with "success at any cost." Modern blockbusters propagate a "beautiful life." Media channels show politics "influenced" by rich people. Money becomes the measurement for achievement and success. It would be difficult to eliminate this pressure-rationalization factor from the fraud triangle.

F. SUMMARY

This chapter provided a review of the literature from several types of documents related to internal control issues and an explanation of the phenomenon of fraud. It discussed internal control basics and several federal legislation as well as the COSO Internal Control framework and fraud management. The author concludes that no one single theory can adequately explain fraud.

Some psychological theories focus on factors within the person while other theories—for example the learning theory—focus on the environment. Even the most advanced fraud triangle theory that effectively combines internal and external factors has room for more development. It seems obvious that the blueprint for an anti-fraud program should involve the overlapping of all theories.

The fraud triangle presents the clearest understanding of the major elements of fraud, which include incentive, opportunity, and rationalization. Opportunity is the weakest link in the fraud triangle because it mostly exploits internal control deficiencies. Effective internal control is absolutely critical in a fraud prevention program.

U.S. legislation is associated with a wide range of documents relating to internal control issues. For the purposes of this project, the most significant legislation are Office of Management and Budget (OMB) Circular A-123 (the latest edition) and the COSO ICIF. These documents will provide tools for developing the "Commander's Guide for Detecting and Deterring Procurement Fraud in Military Units in the Armed Forces of Ukraine."

Chapter III discusses the specifics of financial control in the Ukrainian armed forces, which explicitly rely on professional, external audit only.

THIS PAGE INTENTIONALLY LEFT BLANK

III. THE UKRAINIAN MINISTRY OF DEFENSE CONTROL SYSTEM

A. INTRODUCTION

This chapter introduces the state of governmental financial control in Ukraine. Several concepts of internal control, as previously discussed, are absent in the Ukrainian government or have different meanings. The current financial control system of the armed forces is an unrefined part of the overall governmental control system of Ukraine, which is centralized, expensive, inflexible, and ultimately ineffective.

The internal control system exhibits a managerial style in which many top-level agencies of the Ukrainian Ministry of Defense (MoD) have official responsibility, but where division of responsibility is vague. This confusion hinders even the beginnings of a new control system.

This chapter discusses the organizational structure of the Ukrainian Armed Forces and the existing control network. In addition, the strengths and weaknesses of the Ukrainian control system will be reviewed.

B. THE ORGANIZATIONAL STRUCTURE OF THE UKRAINIAN ARMED FORCES

> There is no alternative to creating a modern, combat-effective, highly professional armed forces capable of reacting quickly and adequately to all present-day challenges. (President and Supreme Commander in Chief Victor Yushchenko, White Book 2007, p.3)

The Ukrainian Armed Forces consist primarily of three main branches: The Land Force, Air Force, and Navy.[9] Total personnel (including 50,000 civilian workers) at the beginning of 2009 were 212,000 (White Book, 2008). The current system of hierarchy and control is depicted in Figure 3.

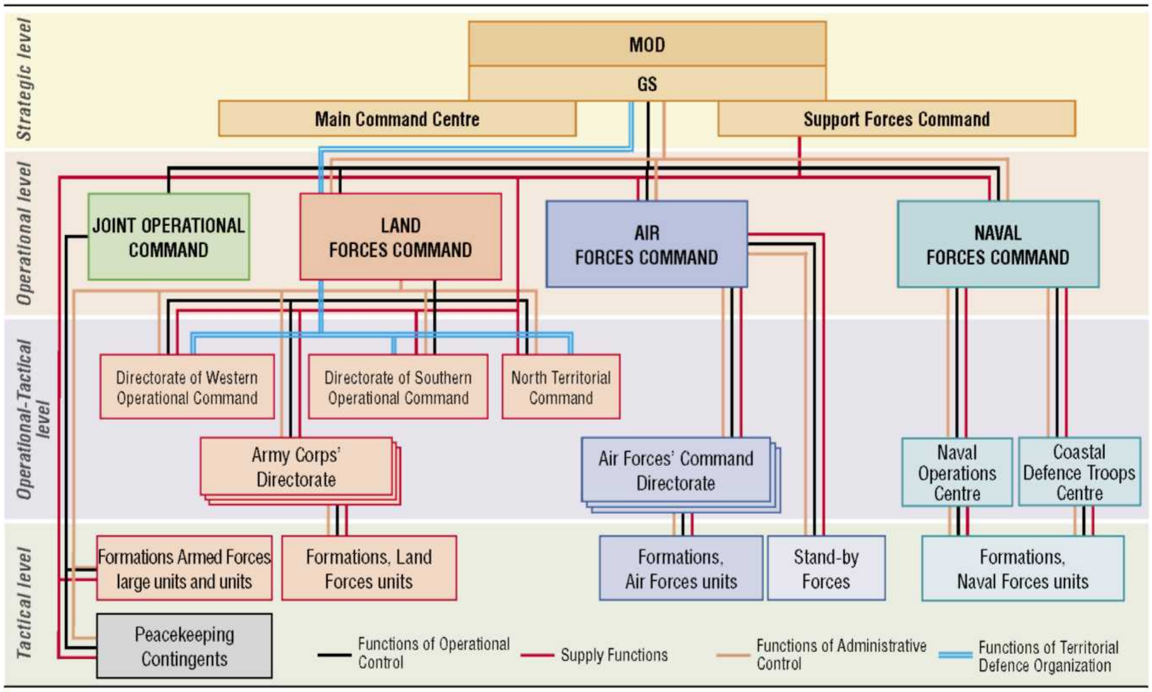

Strategic level
Operational level
Operational-Tactical level
Tactical level
MOD
GS
Main Command Centre
Support Forces Command
JOINT OPERATIONAL COMMAND
LAND FORCES COMMAND
AIR FORCES COMMAND
NAVAL FORCES COMMAND
Directorate of Western Operational Command
Directorate of Southern Operational Command
North Territorial Command
Army Corps' Directorate
Air Forces' Command Directorate
Naval Operations Centre
Coastal Defence Troops Centre
Formations Armed Forces large units and units
Formations, Land Forces units
Formations, Air Forces units
Stand-by Forces
Formations, Naval Forces units
Peacekeeping Contingents
Functions of Operational Control
Supply Functions
Functions of Administrative Control
Functions of Territorial Defence Organization

Figure 3. Command and Control Bodies of the Armed Forces of Ukraine (from White Book 2007)

1. The Land Force of Ukraine

The Land Force was formed by presidential decree in 1996, per Article 4 of the Law of Ukraine, "On the Armed Forces of Ukraine." According to defense doctrine, the land force is the main wielder of combat power (Presidential Decree 648/2004).

From information on the official site of the Ukrainian MoD (http://www.mil.gov.ua), the land force consists of mechanized and armored forces, rocket troops and artillery, land-force aviation, the airmobile force, and air defense for troops. The main command is located in Kyiv.

2. The Air Force of Ukraine

The Air Force was created in 1992 by order of the chief of general staff of the armed forces. This highly mobile branch is assigned to secure national air space by providing full-range air defense, enemy objects assault, landing operations support of Ukrainian troops, military airlift, and aerial reconnaissance (Presidential decree 648/2004).

At present, the Air Force consists of five branches: bomber (Tu-22m3 and Su-24m aircraft), assault (Su-25 aircraft), fighter (Su-27 and Mig-29 aircraft), reconnaissance (Su-24mr and Su-17m4r aircraft), and transport (Il-76 and An-24 aircraft). The main command is in Vinnitsa.

3. The Ukrainian Navy

The Navy defends state interests at sea, eliminating enemy threats in its operational zone alone or in cooperation with the other military forces (Presidential decree 648/2004). The five main branches are surface, submarine, naval aviation, coast rocket-artillery, and Marines. The command is headquartered in Sevastopol.

C. THE EXISTING CONTROL NETWORK

1. Preamble

Before discussing the existing control network, it is necessary to clarify the definitions of several words with different linguistic and conceptual meanings for Ukrainians and Americans.

The term “financial control” in a Ukrainian context differs from its use in the U.S.A. In Ukraine, “control” means “oversight” or “audit.” The difference may appear insignificant, but the reality is not. Financial control in Ukraine does not indicate direct influence on a controlled activity, but rather, a correction of deficiencies or legal violations and the reporting of these problems to management. The main aim of control in Ukraine is to detect possible economic crimes, not to exert influence in organizational activities.

“Internal control” in Ukrainian legislation, administrative usage, and applications is understood as the equivalent of the American “audit.” It refers to controls that are organized within a ministry and does not apply at the entity level. In the Ministry of Defense (MoD), for example, internal control is realized by the control and oversight department, which organizes and provides most of the audits for the MoD. This department has subordinated organizations throughout the services, such as control and oversight offices in Land Force, Air Force, and Navy. Internal control has never played an assurance role or been used as a managerial tool.

The Ukrainian equivalent to the American term “internal control” resembles that of “intra-organizational,” ”intra-economic,” or “managerial” control. However, this type of control in Ukraine has never been assessed as a financial function or had internal audit elements.

2. The Governmental Financial Control System

The legislative branch of the Ukrainian parliament (Verhovna Rada) has financial control functions through the accounting chamber, which “executes control over revenues and expenditures of the state budget of Ukraine on behalf of the Verkhovna Rada of Ukraine.” (Constitution of Ukraine, art. 98)

Governmental financial control through the executive branch is a function of the Ministry of Finance (MF). The MF has two main control structures that directly execute control, and one structure, formerly part of the MF, that is now independent:

- The “Main Control and Revision Office of Ukraine” (though a branch of the MF, its responsibility is equivalent of the U.S. Office of Management and Budget.)
- The “Tax Administration Office” (equivalent to the U.S. Internal Revenue Service, but functioning as a separate central governmental entity—a ministry)
- The “State Treasury of Ukraine” (unlike the American treasury, part of the Ministry of Finance)

a. The Main Control and Revision Office of Ukraine

This office was created under Law of Ukraine “On the Governmental Control and Revision service of Ukraine” in 1993. The office has changed from being an independent governmental office to a branch of the Ministry of Finance, and back again, several times. Although part of the MF, this office has special privileges and authority and an organizational structure that extends territorially over the whole state.

The main tasks of the Main Control and Revision Office are executing control over governmental spending and over financial reporting of ministries, governmental enterprises, and organizations using state budget money, and developing governmental policy in a field of internal financial control (Law of Ukraine No.2939-XII, 1993). The office executes governmental financial control through financial audit, revision of procurement systems, and inspection of governmental organizations (including the armed forces and uniformed services).

b. State Tax Administration of Ukraine

The Tax Administration Office bases its activity on the Law of Ukraine *On the Governmental Taxation Service in Ukraine,* 1990. Like the Main Control and Revision Office, this administrative office fluctuated between being a branch of the MF and a central governmental office. Now it is a separate ministry. Control responsibilities of the office apply to all activities related to taxes, regardless of economic sector or ownership of entities. Because of its narrow and specific objectives, tax control activities within the office have only a minimal relationship to principles of internal control. The office audits military units as well as other organizations to ensure compliance with the tax code.

c. The State Treasury of Ukraine

The State Treasury of Ukraine oversees the budget in crediting proceeds, assuming liabilities, and making payments (Decree of President of Ukraine No. 335, 1995). According to the Resolution of the Cabinet of Ministers of Ukraine No. 1232, 2005, the treasury carries out budget-related activities in various jurisdictions. They perform audit functions to ensure compliance of governmental entities with budget legislation. The treasury also controls spending of budget funds while checking compliance of underlying spending documents with budget allocations and requirements of budget legislation (equivalent of U.S. “color of money”). Finally, the treasury is responsible for insuring compliance of estimates of spending units with the state and local budget lists as well as compliance with unified rules of accounting. The treasury performs audits of military units and other state and local budget-related organizations.

d. Perspectives

Financial control agencies throughout the government are interested in creating effective internal control in organizations as part of assurance services. Accordingly, the Main Control and Revision Office has proposed the development of a state system of internal financial control.

This proposal would change the ideology, practice, and theory of financial control to conform to the "norms and rules of the European Union (EU) and achievements in the legal field in the sphere of state financial control" (Order of the Cabinet of Ministers of Ukraine No. 158-p, 2005). In particular, new concepts would provide for the introduction of "new effective forms of control: internal audit and internal control" (Order of the Cabinet of Ministers of Ukraine No. 158-p. 2005).The proposal establishes a general framework for developing internal control and divides responsibility over the process between governmental offices, laying out a harmonious system of internal audit and internal control using the COSO internal control model.

While this proposal was approved by the cabinet in May 2005, with actual creation and installment of the system projected to occur within five years, no significant progress has been made due to several difficulties. The first difficulty is the absence of basic supportive legislation in the field of internal control. Second, and probably more significant, is the lack of experts and well-trained personnel to understand and implement internal control concepts. The educational system in Ukraine is not presently equipped to produce experts in this discipline because it is a new field that represents a novel departure from past practices. The final difficulty is the engrained thinking of old-fashioned managers who will only consider one form of control--professional inspection-- and will reject any internal control changes.

3. The Financial Control System in the Ministry of Defense

Financial control in the Ministry of Defense (MoD) is a structural part of governmental internal financial control.[10] The importance of the MoD financial control stems from the variety of its subjects and its extended set of regulations. The MoD financial control has a highly centralized structure that follows the general MoD command and control structure (Figure 3.).

The main body of the MoD financial control is the Control and Oversight Department. At the beginning, this department was a structural part of the department of finance. However, in 2001, the MoD decided to separate and expand oversight functions. (MoD Directive No. 170, 2001). Because of ambiguities concerning the current legal basis for financial control inside the MoD, which contains overlapping directives and instructions, in 2002, the ministry tried to divide responsibility over financial control between Control and Oversight and other MoD agencies. As a result, MoD Directive No. D-5, 2002, established Control and Oversight as having the main responsibility over the system of follow-up financial control, which includes audit, inspection, and oversight. Intra-economic" (managerial) control over subordinate units became the responsibility of all top-level agencies of the MoD (Figure 4.). Therefore, internal control functions are dispersed over a wide array of agencies. The Department of Finance assumed responsibility for creating a methodology for preventive financial control over the flow of transactions, the analysis of performance, and financial reporting.

The current organization of financial control in the MoD consists of three levels according to the structure of command and control in the armed forces (Figure 3). At the strategic level of management, Control and Oversight is in charge. At the operational level (the level of main military services), two control and oversight directorates of the Air Force and Navy, respectively,[11] are in place. The army corps, air force commands, and naval centers are administered by about fourteen control and oversight branches[12]. The control and oversight services occupy the total of 230 full-time, professional auditors,[13] seventy-five percent of whom are active-duty, military personnel (mostly senior officers).

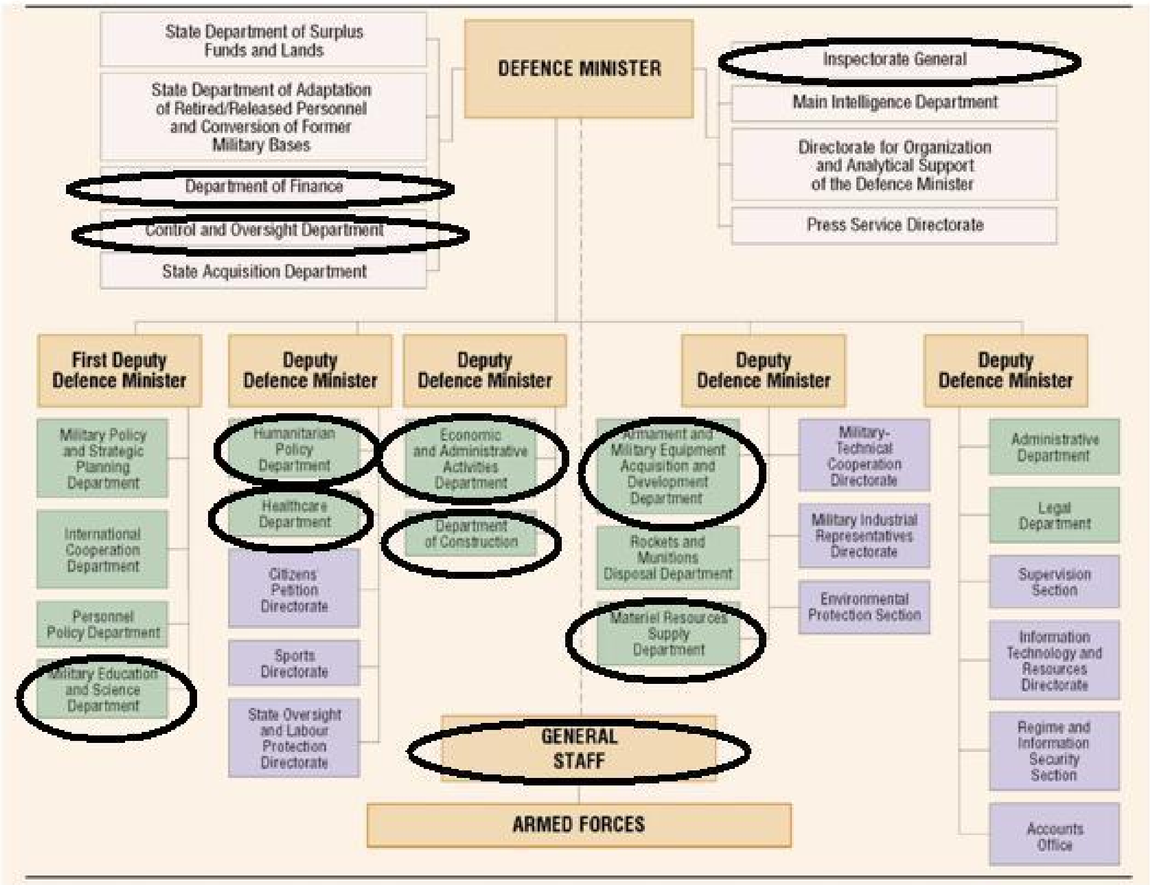

State Department of Surplus Funds and Lands
State Department of Adaptation of Retired/Released Personnel and Conversion of Former Military Bases
Department of Finance
Control and Oversight Department
State Acquisition Department
DEFENCE MINISTER
Inspectorate General
Main Intelligence Department
Directorate for Organization and Analytical Support of the Defence Minister
Press Service Directorate
First Deputy Defence Minister
Deputy Defence Minister
Deputy Defence Minister
Deputy Defence Minister
Deputy Defence Minister
Military Policy and Strategic Planning Department
International Cooperation Department
Personnel Policy Department
Military Education and Science Department
Humanitarian Policy Department
Healthcare Department
Citizens Petition Directorate
Sports Directorate
State Oversight and Labour Protection Directorate
Economic and Administrative Activities Department
Department of Construction
Armament and Military Equipment Acquisition and Development Department
Rockets and Munitions Disposal Department
Materiel Resources Supply Department
Military-Technical Cooperation Directorate
Military Industrial Representatives Directorate
Environmental Protection Section
Administrative Department
Legal Department
Supervision Section
Information Technology and Resources Directorate
Regime and Information Security Section
Accounts Office
GENERAL STAFF
ARMED FORCES

Figure 4. Command-and-Control Central Agencies that Provide Financial Oversight in the Armed Forces of Ukraine (from White Book 2007)

D. STRENGTHS AND WEAKNESSES OF THE UKRAINIAN CONTROL SYSTEM

In system dynamics, the phenomenon of "shifting the burden" is well known. This phenomenon was described by Peter Michael Senge, an American scientist and director of the Center for Organizational Learning at the MIT Sloan School of Management in his *The Fifth Discipline: The Art and Practice of the Learning Organization* (Senge, 1990).

In a "shifting the burden" situation, a problem'*s* symptom can be addressed by applying a symptomatic solution or a more fundamental solution. When a symptomatic solution is implemented, the problem symptom is reduced or disappears. This decreases the pressure for realizing a more fundamental solution. Over time, if a similar symptom arises or recurs, higher level symptomatic solutions are implemented. It is a vicious reinforcing cycle. The symptomatic solutions produce side-effects that take away from the fundamental solutions. (Senge, 1990)

The current financial control organization in the Ukrainian Armed Forces is an obvious case in which the main “control burden” shifted from organizations to top-level management. To respond to increasing fraud within military units during the collapse of the Soviet Union, top-level managers instead of training and developing local control resources, which is a time-consuming process, augmented the capability of central control and oversight agencies. Now, at the top level of the MoD, there are ten agencies that provide financial auditing and are directly responsible for the financial results of military units (see Figure 4, circled data). The question is whether this is an effective or ineffective control structure.

According to Senge (1990), this system should be ineffective because it treats only symptoms, not problems. But the Ukrainian management may argue that the current system has many advantages. First, the current system possesses a high level of expertise. However, highly professional personnel come at a high cost. The professional education of an auditor requires additional time and more resources, which can be quite expensive. The cost of a military auditor who is an officer of the armed forces is about $13,000[14] annually, which is 2.5 times more than the average salary of a Ukrainian military officer of the same rank. Hiring civilian personnel would be less costly for the armed forces organization.

A second argument for the current system is that it is comprehensive. All auditing activity is regulated by directives and instructions that cover almost all possible cases. Though all regulations are static and reactive by definition, fraud and internal control are dynamic systems. New fraud cases and new control responses often are far different from known fraudulent schemes. The reason for that is a continuously changing environment. New regulations can only follow these changes. Moreover, the current environment is uncertain, primarily because of the financial crisis. Managerial control theory holds that uncertainty has powerful repercussions on managerial controls. In uncertain conditions, decentralized control is the most stable option. Decentralized control gives people the ability to act without the delay caused by waiting for directives from the top. As a result, actions to prevent fraud are more timely, pertinent, and flexible.

Finally, the financial control community expresses the idea that the existing financial control system provides absolute assurance of the absence of fraud because of its airtight, overlapping control. In fact, the author's experience shows the opposite to be true because the areas of responsibility among agencies are blurred. For example, the military university is subject to financial auditing from the Control and Oversight Department (general audit of activity), the Economic and Administrative Activities Department (audit of commercial activities), and the Department of Construction (audit of construction activities). The Military Education and Science Department takes general responsibility for university functions and can also audit financial activities. Auditors from different agencies often rely on and refer to information from each other, limiting their own scope of work. Within the school itself, the Military Education and Science Department issues directives about the results of controls and future developments. If fraud is discovered in a past (audited) period, it is impossible to find which auditor neglected the case. As John F. Kennedy observed, "victory has a thousand fathers, but defeat is an orphan."

In summary, the Ukrainian Armed Forces has an intricate, expensive, and ultimately unsatisfactory control system. Following Senge's theory, the solution is to

> Focus on the fundamental solution. If the symptomatic solution is imperative (because of delays in fundamental solution), use it to gain time while working on the fundamental solution. (Senge, 1990, p. 381)

E. SUMMARY

This chapter discussed the current state of financial control in Ukraine, concentrating on specific aspects of the control system as viewed against the organizational structure of the armed forces and the historically inherited controls. This chapter also discussed the organizational structure of the Ukrainian Armed Forces and the existing control network. In addition, the strengths and weaknesses of the Ukrainian control system were reviewed.

The financial control system of Ukraine in general and that of the armed forces in particular do not include internal control as part of a whole, effective system. However, the cabinet has directed the implementation of an internal control system for governmental agencies by approving a COSO internal control model.

Chapter IV applies theoretical concepts of internal control and a criminological understanding of fraud to create an anti-fraud early warning system.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FROM THE EXTERNAL AUDIT SYSTEM TO THE EFFECTIVE INTERNAL CONTROL

A. INTRODUCTION

The need to create internal control systems for Ukrainian military units as official government policy is inevitable. As the new system precipitates organizational and cultural changes, effective leadership becomes extremely important. This research project, culminating in *A Practical Guide for Commanders in Detecting and Deterring Procurement Fraud in Military Units in the Armed Forces of Ukrain*e (hereafter referred to as the *Commander's Guide*), aims to provide both a solid introduction to internal control and guidance in achieving visible, short-term benefits. Because internal control is not a panacea against fraud and must be combined with other external and internal measures, the *Commander's Guide* also informs leaders of the inherent limitations of any internal control system.

This chapter covers the importance of changing leadership strategies to inspire transformational changes in the Ukrainian Armed Forces. Also, the importance of the informational component of an anti-fraud system is discussed in the systemization of fraud cases section of this chapter. Finally, the effectiveness and efficiency of internal control will be addressed.

B. CHANGES IN LEADERSHIP STRATEGIES AND LEVELS OF RESPONSIBILITY

John P. Kotter of the Harvard Business School, widely cited for his research in leadership and management, finds that management functions such as planning and budgeting, organizing and staffing, controlling and problem-solving are important, but not the same as leadership functions such as setting direction, aligning people, and motivating and inspiring (Kotter, 1990). Kotter defines leadership as the process of moving people in a desired direction by “mostly non-coercive means.” Moreover effective leadership moves people in a direction that is “genuinely in their real long-term best interests” (Kotter, 1988).

A feature of effective military organizations is strong leadership, which is about creating, inspiring, and initiating change. To create an internal control system in the MoD, leaders will have to involve themselves in the constant “live” control of execution and performance. This requirement will be contrary to the bureaucratic style of management presently practiced by MoD leadership and thus represents a significant impediment in implementing internal controls.

Bureaucracy implies formal processes, standardization, hierarchy of authority, a focus on written documents, specialization of functions, fixed rules, non-elective government officials, and so on. Bureaucracy was developed to solve problems when the work could be done by people who might not have the skills, experience, motivation, or training to make wide-ranging decisions, but who could do work that was carefully prescribed (McShane, 2007). However, in curtailing a worker’s scope of responsibility through rules and procedures, organizations sacrifice flexibility.

Clearly, the creation of an internal control system is not merely about a new set of rules. It means reformation of an organization’s processes, structure, and culture. The prime task for leadership is developing a strategy to effect positive change.

Kotter (1988) introduces several ideas for leading change. His eight-step program, listed below, combines elements from different disciplines, namely psychology, sociology, economics, and systems thinking.

1. Establish a sense of urgency.

    - Examine market and competitive realities.

    - Identify and discuss crises, potential crises, or major opportunities.

2. Form a powerful guiding coalition.

    - Assemble a group with enough power to lead the change effort.

- Encourage the group to work together as a team.

3. Create a vision.

- Create a vision to help direct the change effort.
- Develop strategies for achieving that vision.

4. Communicate the vision.

- Use every vehicle possible to communicate the new vision and strategies.
- Teach new behaviors by the example of the guiding coalition.

5. Empower others to act on the vision.

- Get rid of obstacles to change.
- Change systems or structures that seriously undermine the vision.
- Encourage risk taking and nontraditional ideas, activities, and actions.

6. Plan for and creating short-term wins.

- Plan for visible performance improvements.
- Create those improvements.
- Recognize and reward employees involved in the improvements.

7. Consolidate improvements and produce still more change.

- Use increased credibility to change systems, structures, and policies that don't fit the vision.
- Hire, promote, and develop employees who can implement the vision.
- Reinvigorate the process with the new projects, themes, and change agents.

8. Institutionalize new approaches.

- Articulate the connections between the new behaviors and corporate success.

- Develop the means to ensure leadership development and succession.

The first lesson from the most successful transformations in corporate America is that the process comprises a series of phases that, in total, usually require a considerable amount of time. Skipping steps creates only the illusion of speed, not the long-term effects leadership desires. A second lesson is that critical mistakes in any one phase can have a devastating impact, slowing momentum, and negating hard-won gains (Kotter, 1988).

Devising a change strategy for creating an internal control system in the MoD is beyond the limits of this project. The aim is to fit the *Commander's Guide* into a general strategic framework for creating internal control, not to prescribe the entire process. It is hoped that this project will help commanders establish a sense of urgency, grasp a vision of the process, and create short-term, visible improvements that will encourage improvements to efficiencies already achieved.

1. Establishing a Sense of Urgency

The first step in the transformational process is critical because it requires aggressive leadership. Without top-level management creating a sense of urgency, people will not help, and the effort will never be successful. Organizational leadership should find ways to communicate this urgency and create opportunities to address the critical elements that created that sense of urgency. The first task outlined in the *Commander's Guide* is a thorough evaluation of the current control system. All deficiencies of internal control in military units and the consequences of those deficiencies must be exposed to create a sense of urgency.

2. Vision

A vision statement clarifies the direction in which an organization needs to move (Kotter, 1990). Without a clear vision, changes can be confusing or insignificant, and policies, instructions, and directives merely become useless paperwork. The second task in the *Commander's Guide* is to create in military leaders a feeling for the overall system of internal control—a grasp of its clear, logical structure, processes, objectives, and subjects—people.

3. Creating Short-Term Benefits

Kotter states that without short-term benefits, too many people give up too soon and begin to resist changes. Short-term gains provide tangible evidence that transformation is working. Short-term gains are important to the overall strategy because when people realize that changes take a significant amount of time, interest decreases. Effective leadership means dedicating a great deal of effort to achieving short-term gains to keep a high level of urgency and support for the vision. For example, successful detection and elimination of discovered fraud should be made highly visible as a short-term gain. Promoting such benefits is the third main goal of the *Commander's Guide*.

4. Shift in Leadership Strategies

The entrenched view among Ukrainian leaders—a legacy of Soviet times—is that people must be coerced into working because they would never choose to do so of their own free will. This assumption no longer works. The model in modern leadership is that people should be intrinsically motivated to perform the tasks requested of them. In general, Ukrainian workers tend to have greater self-esteem now than they did during Soviet Union times. As they become more educated and capable, their employers must take new approaches. Table 2 below summarizes the shift in leadership strategy.

Old Expectations of Leaders	New Expectations of Leaders
• Get results by directing people and getting compliance. • Create strong followers who respect authority. • Get people to follow policy and procedure.	• Facilitators/Process Consultants: managers will need to facilitate the flow of information in groups and between groups. The manager in this role, in addition to attention paid to content, will need to pay close attention to process - the way people work together to accomplish objectives. • Liasons/Linking Pins/Network Builders: formally or informally, managers will be in

• Develop individual strengths within department. • Implement orders for the above (within the organization). • Be responsible for the actions of the work unit. • Be excellent at the technical work performed in the department. • Control people to produce the highest possible output.	a position to bring groups together to solve common problems. Work within groups is constantly affected by actions of external groups with whom the leader should relate. • Integrator/Innovator/Decision Maker: managers must be able to integrate information, conceptualize possible alternatives, and plan productive courses of action. • Conflict Managers/Relationship Builders: as the number of parties involved in problem solving increases, so does the number of different points of view. Leaders need to develop skills to manage conflict productively and build cooperative relationships • Evaluators/Resource Allocators: Helping employees learn to evaluate their own and one another's performance takes time and patience; allocating resources also becomes more challenging when leaders can no longer rely on hierarchical authority to make resource allocation decisions. • Inspirational Leader: leaders will need to help maintain a common vision among different autonomous groups. Leaders will also have to push for exploration of what is possible rather than relying on rules to point the way toward the future." (Pasmore, 1988, p.148)

Table 2. New Leadership Strategies.

C. SYSTEMATIZATION OF FRAUD CASES: A NET-CENTRIC RESPONSE

The net-centric warfare concept, concisely represented by official defense oriented web site *Network Centric Operations Industry Consortium* (https://www.ncoic.org/), is a set of war fighting concepts and capabilities that allow warfighters to take full advantage of all available information and bring all available assets to bear in a rapid and flexible manner. Information in this concept plays the most crucial role.

To create informational advantage, discovered fraud cases need to be systematized and analyzed for both training purposes and for detecting similar fraudulent schemes. An effective systematization of fraud cases for educational purposes is given in the Association of Certified Fraud Examiners' (AFCE's) *Report to the Nation*. The 2008 *Report* studies 959 cases of occupational fraud in the United States, which can be applied to similar situations in Ukraine, and in the Armed Forces organizations, specifically. The study found some interesting trends, classifying occupational fraud into three major categories (Figure 5):

- Asset misappropriation, which involves larceny or misuse of an organization's assets
- Corruption, which includes kickbacks, bid-rigging, and hidden business interests in vendors
- Fraudulent financial statements, which includes overstating revenues and understating liabilities and expenses

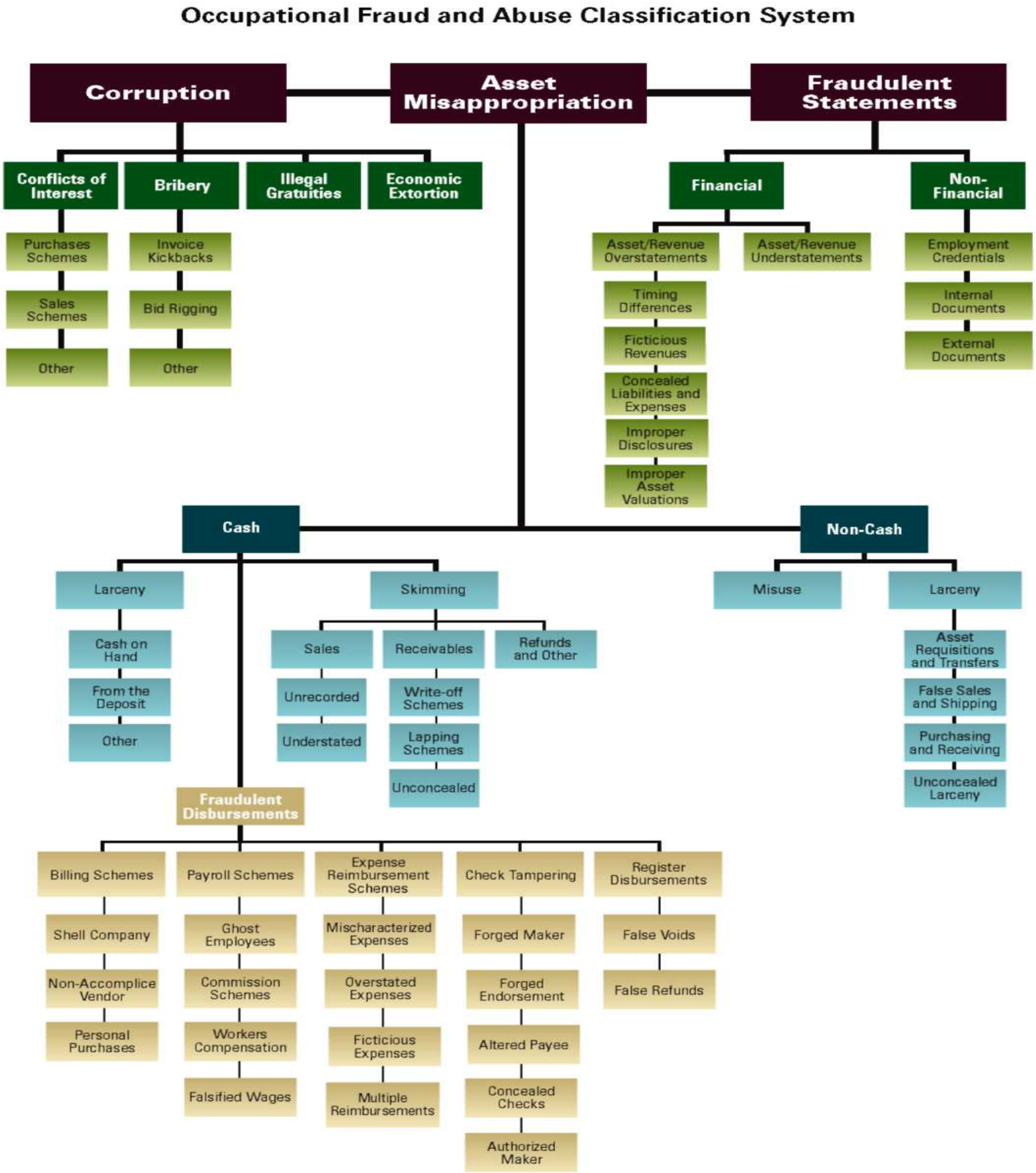
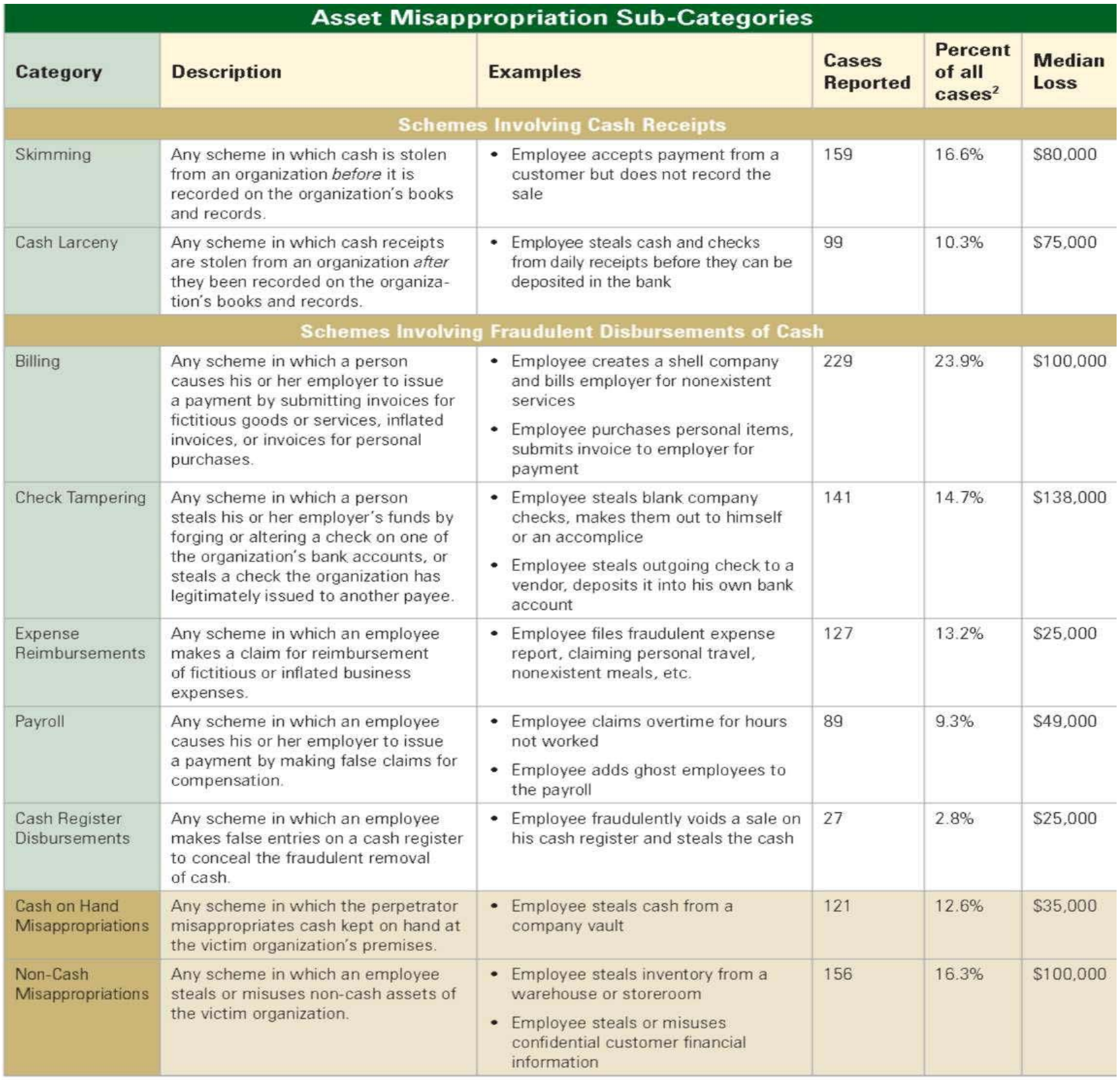


Figure 5. Occupational Fraud and Abuse Classification System (from ACFE, 2008)

Asset Misappropriation is involved in 91.5% cases of all fraudulent activity with median losses of $150K (ACFE, 2008). The ACFE subdivides asset misappropriation schemes into nine categories (Table 3).



Asset Misappropriation Sub-Categories

Category	Description	Examples	Cases Reported	Percent of all cases[2]	Median Loss
Schemes Involving Cash Receipts					
Skimming	Any scheme in which cash is stolen from an organization *before* it is recorded on the organization's books and records.	• Employee accepts payment from a customer but does not record the sale	159	16.6%	$80,000
Cash Larceny	Any scheme in which cash receipts are stolen from an organization *after* they been recorded on the organization's books and records.	• Employee steals cash and checks from daily receipts before they can be deposited in the bank	99	10.3%	$75,000
Schemes Involving Fraudulent Disbursements of Cash					
Billing	Any scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases.	• Employee creates a shell company and bills employer for nonexistent services • Employee purchases personal items, submits invoice to employer for payment	229	23.9%	$100,000
Check Tampering	Any scheme in which a person steals his or her employer's funds by forging or altering a check on one of the organization's bank accounts, or steals a check the organization has legitimately issued to another payee.	• Employee steals blank company checks, makes them out to himself or an accomplice • Employee steals outgoing check to a vendor, deposits it into his own bank account	141	14.7%	$138,000
Expense Reimbursements	Any scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses.	• Employee files fraudulent expense report, claiming personal travel, nonexistent meals, etc.	127	13.2%	$25,000
Payroll	Any scheme in which an employee causes his or her employer to issue a payment by making false claims for compensation.	• Employee claims overtime for hours not worked • Employee adds ghost employees to the payroll	89	9.3%	$49,000
Cash Register Disbursements	Any scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash.	• Employee fraudulently voids a sale on his cash register and steals the cash	27	2.8%	$25,000
Cash on Hand Misappropriations	Any scheme in which the perpetrator misappropriates cash kept on hand at the victim organization's premises.	• Employee steals cash from a company vault	121	12.6%	$35,000
Non-Cash Misappropriations	Any scheme in which an employee steals or misuses non-cash assets of the victim organization.	• Employee steals inventory from a warehouse or storeroom • Employee steals or misuses confidential customer financial information	156	16.3%	$100,000

Table 3. Assets Misappropriation Classification (from ACFE, 2008).

Statistics show that a majority of fraud cases involve cash. As seen in Table 3, eight of nine categories are cash related, and fraudulent disbursements are the most popular form of cash schemes. Procurement billing schemes are most commonly involved. The idea of using a structured fraud analyzing process for assessing new cases is similar to the process of malware detection in computer science and inspired the author to research a computer antivirus strategy for building an anti-fraud system.

Following computer science approaches, an analogy between computer viruses (malware) and fraud can be made. Computer malware and fraud have many similarities including negative outcomes, malicious intent, hidden behaviors, distorted reasoning, and so on. As engineers and mathematicians, the computer scientists who produce antivirus software seek clear, straightforward solutions. Their strategies can be extrapolated and used to combat fraud. The following ideas from this field are extremely valuable:

- **Antivirus strategies imply a sequence of actions.** All actions have equal importance and must be done in proper order, without omission. The optimal order consists of (1) examining for viruses using a virus dictionary, (2) identifying suspicious behavior from any process or computer program that can indicate infection (heuristic analysis), (3) placing resident controls in the system, (4) monitoring control system integrity, and (5) periodically scanning the whole system.
- **An antivirus system must be flexible.** The best antivirus systems contain several independent but interrelated modules. Each module provides a discrete aspect of control and can be added or switched off depending on user resources, control objectives, and the required level of security. Tighter control demands greater resources, such as computer memory or central processor capability.
- **A control system should be as dynamic as possible.** Modern antivirus systems update their dictionary of known viruses and their software on a daily or hourly basis.

Analogically to antivirus software, a fraud prevention program needs to start with an analysis of the probability that fraud already has occurred in the organization. All crucial internal control elements are based on managers' integrity. There is always the possibility of management override of the internal control system. Therefore, similarly to antivirus software, the environment needs to be scanned for potential fraud. Appropriate additional "heuristic" analysis of suspicious behavior would also be an effective tool. All of these elements can be used in an anti-fraud program. However, even the most effective internal control program is not free from limitations.

D. EFFECTIVENES AND EFFICIENCY OF INTERNAL CONTROL (COST-BENEFIT ANALYSIS)

There are several factors that can limit internal control, which include internal control complexity and excessive cost. Each of these factors can be a barrier to the effective control of an organization. Being aware of these factors aids leadership in maximizing the effectiveness of an operation, whether in a governmental or corporate environment.

Complicated internal control measures can be misunderstood by employees who are fatigued or exercise poor judgment (Whittington & Pany, 2008, p. 256). Although a complex internal control system is feasible in theory, actual measures may be too cumbersome to be practical. The result of complex, all-embracing systems may be confusion and misunderstanding.

Even a sound internal control system can be cost ineffective if its costs outweigh its value to operations. Therefore, in a non-fraud environment, management tends to discard internal controls. Since a perfect control system is expensive and could produce a non-optimal output, and a cost-efficient control system is unable to significantly decrease fraud risk, there is a cost dilemma. The optimal internal control system should benefit the organization at a reasonable cost, a compromise which is difficult to achieve. Recognizing that control measures provide reasonable rather than absolute assurance in addition to the possibility of management's overriding any control measures are important limiting factors to consider. (Whittington & Pany, 2008).

The relevancy (or efficiency) of internal controls must be discussed. As Bradford Cadmus and Arthur J. E. Child, authors of *Internal Control Against Fraud and Waste,* observe,

> Even though a certain control measure is possible, it may not be necessary or desirable. Every measure of control should meet these tests: Does it control something that is worthwhile to control? Are minor items rigidly controlled because such control is feasible, while major items are less rigidly controlled because control is harder to establish? Does it meet protective requirements on a practical basis? Whether it be a petty cash fund, a storeroom, or a variety chain store, the complication and cost of

> protective control must be appraised in relation to possible exposure to fraud, waste, or loss. Is it flexible to meet changing business conditions? (Cadmus & Child, 1953, p. 305).

However, the effectiveness of an internal control system is mostly measured arbitrarily by leadership/management judgment. The ultimate measure of effectiveness should not be the cost, but the capability of providing reasonable assurance that control objectives have been met (see Chapter II for definition of control objectives).

E. SUMMARY

This chapter has underscored the relevancy of the Ukrainian military leaders who will play a crucial role in control-system transformation. It discussed the significance of the informational component of an anti-fraud program as well as the systemization of fraud cases. In addition, the effectiveness and efficiency of internal control were addressed. The implementation of a fraud management system at the organizational level in the Ukrainian Armed Forces would be a great benefit.

The guidelines provided in the *Commander's Guide* should enable personnel to use the document as a template for creating other guides, for preventing payroll fraud, skimming, check tampering, etc.

The inherent limitations of an internal control system are important to understand and should be factored in during the system design phase. An internal control system should be relevant to its objective. Excessive control often brings confusion and misunderstanding, in addition to extra cost.

Chapter V provides the actual *Commander's Guide*.

V. A COMMANDER'S (OR EXECUTIVE OFFICER'S) GUIDE FOR DETECTING AND DETERRING PROCUREMENT FRAUD IN A MILITARY UNIT (OR ORGANIZATION) OF THE ARMED FORCES OF UKRAINE

A. INTRODUCTION

The Association of Certified Fraud examiners' (ACFE) fraud examiner's manual states that fraud prevention demands a system of rules and action in order to minimize the possibility of fraud occurring and maximize the possibility of detecting any fraudulent activity. The manual states that the "potential of being caught most often persuades likely perpetrators not to commit the fraud. Because of this principle, the existence of a thorough control system is essential to fraud prevention." (*Fraud Examiner's Manual*, 2007, p.4.601)

The key words here are "the potential of being caught" and "the existence of a thorough control system"—two main elements critical in any effective fraud prevention program.

This suggested *Commander's Guide* includes procedures and guidelines that could be helpful in deterring and detecting fraud and in establishing an anti-fraud prevention program. It is recommended that the commander create a fraud investigating team or task force to conduct the recommended anti-fraud activities. This task force is a key element of an anti-fraud program.

The fraud task force should perform fraud detection procedures using the fraud indicator guidelines presented in this chapter. The creation and development of effective internal controls demand significant resources, time, and training before first-time basic procedures can be put in place. This guide will provide examples of anti-fraud internal control elements. Section B will provide fraud indicator guidelines. Section C will discuss guidelines for a basic fraud prevention program. Section D will cover guidelines for establishing an advanced anti-fraud internal control system. Section E includes a procurement fraud dictionary. Section F includes a summary of the detailed guidelines.

B. FRAUD INDICATOR GUIDELINES

These guidelines suggest three consecutive steps to mitigate fraud. First, fraud can be detected by analyzing suspicious behavior or actions. Second, if fraud is detected, the fraud investigating team should perform the appropriate actions to investigate the fraudulent activity more thoroughly and to prevent the concealment of facts. Third, to resolve fraud cases, the commander should take disciplinary and legal actions against fraud perpetrators.

1. Fraud Detection

There are four major types of indicators that suggest fraudulent activity: situational, accounting, documentary, and behavioral.

Situational Indicators: (adapted from the United States Agency for International Development (USAID) *Fraud Indicators Handbook*, 2009).

a. Procurement Planning

- Continual vacillation about what an organization wants or inadequate development of a needs assessment
- Requiring excessively high stock levels and inventories in order to justify continuing purchasing activity from certain contractors
- Declaring serviceable items as excess or selling them as surplus while continuing to purchase similar items
- Purchasing items and services in response to aggressive marketing efforts (and possible favors, bribes. or gratuities) by contractors rather than in response to valid requirements

b. Solicitation Phase

- Using statements of work, specifications, or sole-source justifications developed by or in consultation with a preferred contractor (institutional conflict of interest)
- Bid specifications or statements of work are not consistent with the items included in the general requirements
- Falsified statements to justify sole source of negotiated procurement
- Placing unnecessary restrictions in solicitation documents (confidentiality, etc.), which could tend to restrict competition
- Limiting the time for submission of bids so that only those with advance information have adequate time to prepare bids or proposals
- “Referring” a contractor to a specific subcontractor, expert, or source of supply. Expressing or implying that using the referred business will more than likely secure the contract
- Improper acceptance of late bids
- Changes in a bid after other bidders’ prices are known. This is sometimes done by deliberately “planting” mistakes in a bid
- Falsification of information concerning contractor qualifications, financial capability, qualifications of personnel and successful performance of previous jobs, etc.
- Seemingly unnecessary personal contacts between involved managers and contractor’s personnel during the solicitation, evaluation, and negotiation processes
- Using biased evaluation criteria or biased individuals on the evaluation panel

- Dealing with oddly-named vendors which suggests that the firm may not provide the type of service or product being solicited

c. Source Selection

- Award of a contract to a contractor who is not the lowest responsible, responsive bidder
- Material changes in the contract shortly after award
- Awards made to contractors with an apparent history of poor performance
- Awards made that include items other than those contained in bid specifications
- Backdated or after-the-fact justifications in the contract file or contracts signed by persons without the authority to approve noncompetitive procurement

d. Contract Administration

- Certified receipt of goods and services even though physical inspections have not been performed
- Contractors failing to meet contract terms but nothing done to enforce compliance
- Fictitious or inordinate time frames and dates on contractor records (e.g. gasoline, vehicle, maintenance, inspection, or receiving reports).
- Excessive or insufficient freight expense relative to inventory purchased or to sales. May indicate that purchases have been paid through means not reflected on the books or inventory purchased or sales made for unrecorded cash
- Used or inferior products substituted for product actually ordered

- Significant increase in power consumption in a manufacturing facility without a corresponding increase in production or revenue
- Using cash to pay vendors instead of relying on electronic bank systems

Accounting Record Indicators: (adapted from the American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) No 99).

- Transactions not recorded in a complete or timely manner or improperly recorded as to amount, period, or budget classification code
- Purchased items not recorded in inventory records
- Unsupported or unauthorized transactions
- Last-minute or unauthorized adjustments

Documentary (Source Documents) Indicators: (adapted from AICPA SAS No 99 and Inspector General Shell Company and Suspect Purchases, 2009).

- Missing electronic or hardcopy documents that "materialize" later in the review
- Availability of only photocopied documents instead of original documents. Copies are poor quality or illegible. It is a simple matter to alter approved invoices with white-out or similar correction fluid and copy the invoice while destroying the original.
- Out-of-sequence invoices in files or unnumbered invoices where serial numbering is the rule
- Documents from competing firms containing similar or identical company names, handwriting/signatures, stationery, invoice numbers (in sequence), telephone numbers
- Significant unexplained items on reconciliations
- Inconsistent, vague, or implausible accounting reports or analytical documents sent to different organizations

- Unusual discrepancies between computer report totals and source documentation. Missing signatures of approval.
- Discrepancies between accounting records and confirmation replies

All of these indicators must be assumed as red flags, reported to the oversight agency, and investigated accordingly.

Behavioral Indicators: Employee behaviors may indicate fraudulent activity. Two groups of indicators that can be used for detection of fraud include behavior that shows a high probability that a fraud has occurred and employee incentives and reasons to commit the fraud. Behavior that shows a **high probability** of fraud (adopted from Whittington & Pany, 2008) include:

- Denial of access to records, facilities, certain employees, customers, vendors, or others related to possible evidence
- Complaints by management about the conduct of the audit or management intimidation of auditors
- Unusual delays by the entity in providing requested information
- Tips or complaints to the auditors about fraud from employees
- Unwillingness or denial of access to key electronic files for testing

In addition to the above indicators, there are three conditions or factors that are generally present when fraud occurs. First, management or employees will have an **incentive** or **situational pressure** that provides a reason to commit fraud. Second, the **opportunity** for a fraud will exist, caused mostly by the absence of controls or the ability of management to override controls. Third, **lack of personal integrity** or the ability to **rationalize** committing a fraudulent act will generally also be present.

Fraud is usually found if there is a negative balance of all these factors (Figure 6). Elimination of only one will not stop fraud if critical levels of other factors outweigh it.

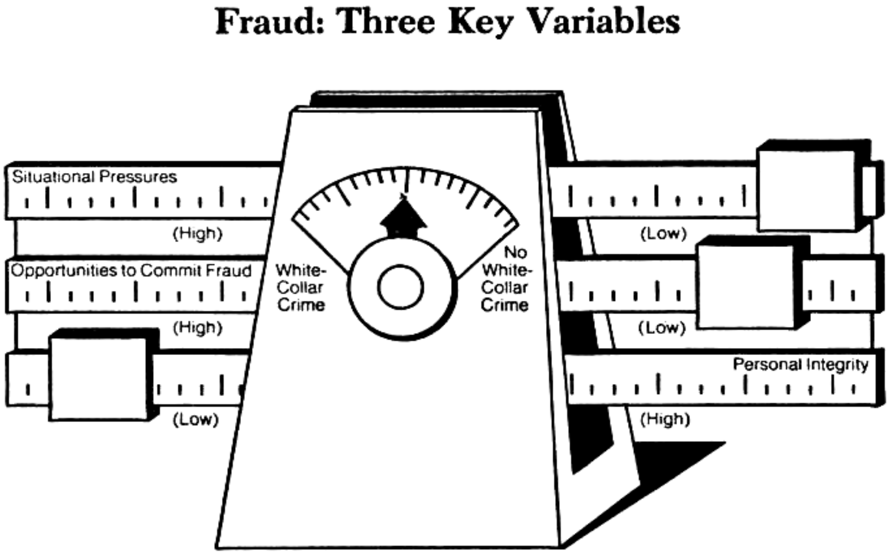


Figure 6. Three key variables model of fraud (from Albrecht et al., 1982, p 39)

(1) <u>Situational Pressures:</u> (adapted from Albrecht et al., 1982)

There are many motivations for fraud, most related to greed, such as living beyond one’s means, having an immediate financial need, possessing debts, poor credit, and a drug or gambling addiction, and experiencing family pressure. While this list is not inclusive, answers to these questions can help identify fraud perpetrators:

- Do any involved employees have unusually high personal debts or financial losses that probably exceed their level of income?
- Do the incomes of any key employees appear inadequate to cover normal personal and family expenses?
- Do any key employees appear to be living beyond their means?
- Are any key employees involved in extensive FOREX, stock market, or other speculation so that a downturn would cause severe financial difficulty?
- Are any key employees involved in excessive or habitual gambling?

- Do any key employees have unusually high expenses resulting from personal involvement with other people, especially the opposite sex (e.g., maintenance of separate apartments)?
- Do any key employees feel undue family, community, or social expectations or pressures?
- Do any key employees use alcohol or drugs excessively?
- Do any key employees strongly believe that they are being treated unfairly (e.g., underpaid, poor job assignments)?
- Do any key employees appear to resent their superiors?
- Are any employees unduly frustrated with their jobs?
- Is there an undue amount of pressure for employees to achieve in this organization, so that success is more important than ethics?
- Do any key employees appear to exhibit extreme greed or an overwhelming desire for self-enrichment or personal gain?

(2) Opportunities: (adapted from Albrecht et al., 1982, Broader, 2000, COSO *Internal Control—Integrated Framework*, 1992, and GAO-01-1008G, 2001).

Weak internal control is the crucial factor that creates opportunity for fraud. The following are questions at the organizational level. While this list is not inclusive, answers to these questions can help identify fundamental internal control weaknesses.

- Are there codes of conduct or ethics policies?
- Do control systems test for compliance with codes of conduct?
- Does the organization inform employees about rules of personal conduct and the discipline meted out to fraud perpetrators?
- Are the accounting department and other key structures of the organization adequately staffed?

- Is it easy to recognize management’s leadership philosophy and operating style?
- Do formal subordinate manager-employee relations prevail over the informal relations?
- Do human resource policies and practices contain rules and incentives for honest behavior?
- Is there an adequate anti-fraud training program for employees?
- Do any key employees have close associations with suppliers/contractors or individuals who might have motives inconsistent with the organization’s welfare?
- Have any key employees recently failed to take annual vacations?
- Does the organization have adequate personnel screening policies when hiring new employees to fill positions of trust?
- Are executive disclosures of personal investments or incomes required?
- Is the organization dominated by only one or two individuals?
- Does the organization appear to operate continually on a crisis basis?
- Does the organizations place too much trust in key employees?
- Does the organization lack a good system of internal security (e.g., locks, safes, fences, gates, and guards)?
- Is the organization highly computerized? If so, are there sufficient controls over hardware, software, computer personnel, etc.?
- Do policies and procedures ensure critical decisions are made with appropriate approval?
- Are key risk-taking activities appropriately segregated from reconciliation activities?

- Do all personnel understand their accountability for the activities they conduct?

(3) Rationalizations and Personal Integrity: (adapted from Albrecht et al.,1992).

The next list of questions suggests a set of rationalizations that define the fraudulent behavior most likely to occur in a given situation. While this list is not inclusive, answers to these questions can help identify people likely to commit fraud.

- Do any of the key employees appear to have low moral character?
- When confronted with difficulty, do any of the key employees appear consistently to rationalize contradictory behavior?
- Do any of the key employees appear to lack a strong personal code of honesty?
- Do any key employees appear to be "wheeler-dealer" individuals who enjoy feelings of power, influence, social status, and excitement associated with financial transactions involving large sums of money?
- Do any of the key employees appear to be unstable (e.g., frequent job changes or changes of residence, mental problems)?
- Do any key employees appear to be intrigued by the personal challenge of subverting a system of controls (i.e., a desire to beat the system)?
- Do any key employees have criminal or questionable backgrounds?
- Do any employees have poor credit ratings?
- Do any employees have poor past work records or references?

2. Follow-Up Detection Procedures

If a fraud investigative unit identifies a red flag, it should change and/or extend the auditing procedures. Some helpful examples of extra procedures are the following (not inclusive):

- Observe inventory on unexpected dates or at unexpected locations, or count cash on a surprise basis
- Examine the data for the same vendor, amount, and date (duplicate information to allow for vendor submitting the same invoice but changing the invoice number).
- Compare check numbers against dates issued. Checks should be issued in sequence by check number and date.
- Check for differences in addresses, such as slightly different or incorrect post office boxes and different postal codes for the same address, different street numbers, or alternating addresses.
- Look for checks to different vendors going to the same mailing address.
- Look for checks to different vendors deposited in the same bank account.
- Examine the data for split purchases (transactions on the same day to the same vendor, transactions in round amounts (e.g., $100, $300, or just slightly below the established micro purchase threshold).
- Compare the purchase order date and the invoice date for after-the-fact purchases.
- Interview personnel involved in activities in areas where a risk of material misstatement due to fraud has been identified to obtain their insights about the risk and how controls address the risk.
- Report to the Control and Oversight Department and ask for a professional audit.
- Establish lock-and-key control procedures for audited documentation and data to prevent unauthorized access of fraud-involved personnel.
- Suspend or reassign employees suspected of fraudulent activity.

3. Fraud Resolution

Any action taken should be appropriate under the circumstances and applied consistently to all levels of employees, including senior management. Possible actions include one or more of the following (adapted from the Institute of Internal Auditors, 2008):

Criminal Referral. The organization may refer the case to law enforcement according to the criminal code of Ukraine. Referrals for criminal prosecution may increase the deterrent effect of a fraud prevention policy.

Civil Action. The organization must pursue its own civil action against the perpetrators to recover funds.

Disciplinary Action. The organization must take internal disciplinary action according to service regulations for military offenders and termination, demotion, or warnings for civilians.

Extended Investigation. The Control and Oversight Department is responsible for conducting a root-cause analysis and extended investigation. It can identify similar misconduct elsewhere in the organization.

Internal Control Remediation. The organization should step up internal control activities through either a basic fraud prevention program or an advanced anti-fraud internal control program, depending on the resources available and time limitations.

C. GUIDELINES FOR A BASIC FRAUD PREVENTION PROGRAM

1. Fraud Task Force

To provide a first-time fraud checkup, a unit’s commander should create a temporary or permanent fraud investigation unit that will be responsible for the detection, investigation, and prevention of fraud. It is strongly encouraged that senior management be represented on this team. The chief financial officer should lead this unit. The fraud investigation unit should have a mission statement that provides clear objectives.It is better to use language with positive connotations when naming the team: “financial integrity” rather than “control”, “audit,” or “investigation” team. The team should include both senior management and professionally trained or experienced financial control systems people.

2. Whistle-Blower Programs and Anti-Fraud Hotlines

The American experience teaches that fraud is often uncovered and exposed by people with inside knowledge, including employees, suppliers, and customers. Tips from employees are the most common source of fraud detection, and hotlines are the reporting mechanism of choice. (ACFE, 2008)

The ACFE (2008) found that tips were the most common way frauds were detected, far more often than through internal or external audits or internal control systems. Tips uncovered 46.2 % of fraud cases, while internal audits accounted for 19.4% and external audits only 9.1%. In addition, most tipsters are employees (ACFE, 2008).

It is easy to say that a commander should support whistle-blowers. In reality, however, members of the military community in Ukraine traditionally do not use positive terms when referring to those who blow the whistle on fraud and abuse. Rather, they are deemed rats, snitches, betrayers, and worse.

To avoid negative employee attitudes towards the program, the following suggestions by Biegelman & Bartow (2006) would be useful for setting up hotlines:

- Choose the right name. Instead of the standard term “hotline,” a less threatening title such as an “aware line,” “advice line” or “integrity helpline” may be in order.
- The hotline number must be easily accessible.
- The number must be toll free.
- The hotline must be available twenty-four hours a day, seven days a week.
- Maintaining the confidentiality and anonymity of hotline callers is absolutely critical to the success of the hotline. Confidentiality means that the caller’s identity and information will not be communicated broadly to

those without a need to know, while anonymity provides secrecy and nondisclosure of the caller’s identity, but not the information obtained.

- The hotline must be staffed by live people versus computer generated voice responses
- The caller should be advised that the calls are not recorded or traced.
- Hotlines should take calls covering all kinds of wrongdoing: fraud, abuse, corruption, theft, sexual harassment, workplace violence, and other violations. (Biegelman & Bartow, 2006)

Potential reporters of fraud should have as many communication channels available as possible to report fraud: telephone, e-mail, letter, and fax. Another basic recommendation for helping to deter and detect fraud is an anti-fraud training program.

3. Anti-Fraud Training

Fraud prevention begins with training. Training should be required for all employees, from the executive level down, and should cover code of conduct, risk of fraud, and the employee’s role in preventing fraud.

There are many ways to deliver quality training including professional seminars, internet-based, interactive training modules, and postgraduate courses. Because organizations are usually limited in their training budget, it is better to provide training programs separately, according to the organizational level in which personnel are involved in the actual fraud preventive program. Fraud investigators (task forces) should be trained externally by certified professionals, and in turn may provide in-house training for managers and employees. Using a task force for educating employees has the additional preventative benefits of showing potential fraud perpetrators that there is a professional investigative unit within the organization and of sending an important message that improper conduct has consequences and will not be tolerated.

As Kenneth R. Dieffenbach, CFE, suggests a basic fraud awareness training for employees, which should include the following basic elements:

- Give a simple definition of fraud: fraud is lying, cheating, and stealing from the organization.

- Discuss how fraud negatively impacts a company's bottom line and reputation.

- Give examples of various fraud schemes employees might discover, such as an offer for kickbacks or the illegal use of customers' credit-card numbers by other employees.

- Tell employees what they are supposed to do if they suspect a fraud. (as cited in Biegelman & Bartow, 2006, p.298.)

One more effective training approach is setting a good example for others to follow. Good leaders are always role models for their subordinates, providing guidance, mentoring, and giving examples of honesty and integrity. Such behavior has a great impact on preventing fraud.

Biegelman & Bartow(2006) suggest providing separate, more detailed, anti-fraud training for managers for two reasons. First, the credibility of the "tone at the top" begins with a unit's first-line leaders. Second, managers need a broad understanding of the kinds of internal and external frauds that can attack an organization.

D. GUIDELINES FOR ESTABLISHING AN ADVANCED ANTI-FRAUD INTERNAL CONTROL PROGRAM

The following guidelines for establishing an advanced anti-fraud internal control program in military units and organizations is adapted from the U.S. General Accounting Office's publication for internal control standards, *Internal Control Management and Evaluation Tool*, GAO-01-1008G, 2001. It will cover the five components of an internal control system, which include the control environment, risk assessment, control activities, information and communication, and monitoring.

1. The Control Environment

Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.

a. *Integrity and Ethical Values*

(1) The organization should establish and use a formal code of conduct and other policies communicating appropriate ethical and moral behavioral standards. Consider the following:

- The codes are comprehensive in nature and directly address issues such as improper payments, appropriate use of resources, conflicts of interest, and use of due professional care.
- The codes are periodically acknowledged by signature from all employees.
- Employees indicate that they know what kind of behavior is acceptable and unacceptable, what penalties unacceptable behavior may bring, and what to do if they become aware of unacceptable behavior.

(2) An ethical tone should be established at the top of the organization. Consider the following:

- Management fosters and encourages an organizational culture that emphasizes the importance of integrity and ethical values. This might be achieved through different media: intranet, oral communications in meetings, via one-on-one discussions, and by example in day-to-day activities.
- Employees indicate that peer pressure exists for appropriate moral and ethical behavior.
- Management takes quick and appropriate action as soon as there are any signs that a problem may exist.

(3) Dealings with the external organizations and employees should be conducted on a high ethical level. Consider the following:

- Management cooperates with auditors and other evaluators, discloses known problems to them, and values their comments and recommendations.
- The organization has a well-defined and understood process for dealing with employee claims and concerns in a timely and appropriate manner.

(4) Appropriate disciplinary action should be taken in response to departures from approved policies and procedures or violations of the code of conduct. Consider the following:

- Management takes action when there are violations of policies, procedures, or the code of conduct.
- The types of disciplinary actions that can be taken are widely communicated throughout the organization so that others know that if they behave improperly, they will face similar consequences.

(5) Management should appropriately address intervention or overriding of internal controls. Consider the following:

- Any leadership decision about intervention or overriding of internal control is fully documented as to reasons and specific actions taken.
- Overriding of internal control by low-level management personnel is prohibited except in emergency situations Upper-level management is immediately notified and the circumstances are documented.

(6) Management should remove temptation for unethical behavior. Consider the following:

- Management has a sound basis for setting realistic and achievable goals and does not pressure employees to meet unrealistic ones.
- Management provides fair, non-extreme incentives (as opposed to unfair and unnecessary temptations) to help ensure integrity and adherence to ethical values.
- Compensation and promotion are based on achievements and performance.

b. Commitment to Competence

(1) Management should identify and define the tasks required to accomplish particular jobs and fill the various positions. Consider the following:

- Management has analyzed the tasks that need to be performed for particular jobs and given consideration to such things as the level of judgment required and the extent of supervision necessary.
- Formal job descriptions or other means of identifying and defining specific tasks required for job positions have been established and are up to date.

(2) The organization should perform analyses of the knowledge, skills, and abilities needed to perform jobs appropriately. Consider the following:

- The knowledge, skills, and abilities needed for various jobs have been identified and made known to employees.

- Evidence exists that the agency attempts to assure that employees selected for various positions have the requisite knowledge, skills, and abilities.

(3) The organization should provide training and counseling in order to help employees maintain and improve their competence for their jobs. Consider the following:

- There is an appropriate training program to meet the needs of all employees (if it is not feasible to provide such program at the organizational level, the management must ask for help from the parent organization or agency).
- Performance appraisals are based on an assessment of critical job factors and clearly identify areas in which the employee is performing well and areas that need improvement.
- Employees are provided candid and constructive job performance counseling.

(4) Key senior-level employees should have a demonstrated ability in general management and extensive practical experience in operating governmental or business entities.

c. Management's Philosophy and Operating Style

(1) Unit (organization) leadership should have an appropriate attitude toward risk taking and proceeds with new ventures, missions, or operations only after carefully analyzing the risks involved and determining how they may be minimized or mitigated.

(2) Management should enthusiastically endorse the use of performance-based management.

(3) There should not be excessive personnel turnover in key functions, such as operations and program management or accounting. Consider the following:

- There has not been excessive turnover of supervisory personnel related to internal control problems, and there is a strategy for dealing with turnover related to constraints and limitations such as salary caps.
- Key personnel have not quit unexpectedly.
- Personnel turnover has not been so great as to impair internal control as a result of employing many people new to their jobs and unfamiliar with the control activities and responsibilities.
- There is no pattern to personnel turnover that would indicate a problem with the emphasis that management places on internal control.

(4) Management should have a positive and supportive attitude toward the functions of accounting, information management systems, personnel operations, monitoring, and internal and external audits and evaluations. Consider the following:

- The financial accounting and budgeting operations are considered essential to the well-being of the organization and viewed as methods for exercising control over the entity’s various activities.
- Management regularly relies on accounting/financial and programmatic data from its systems for decision-making purposes and performance evaluation.

- If the accounting operation is decentralized, unit accounting personnel also have reporting responsibility to the central financial officer(s).
- The financial management, accounting operations, and budget execution operations are under the direction of the chief financial officer, and strong synchronization and coordination exists between budgetary and proprietary financial accounting activities.
- Management looks to the information management function for critical operating data and supports efforts to make improvements in the systems as technology advances.
- Personnel operations have a high priority and senior executives emphasize the importance of good human-capital management.
- Management places a high degree of importance on the work of the external audits from the Control and Oversight Department of the MoD or other governmental oversight structures as well as other evaluations and studies and is responsive to information developed through such products.

(5) Valuable assets and information should be safeguarded from unauthorized access or use.

(6) There should be frequent interaction between senior management and operating/program management, especially when operating from geographically dispersed locations.

(7) Management should have an appropriate attitude toward financial, budgetary, and operational/programmatic reporting. Consider the following:

- Management is informed and involved in critical financial reporting issues and supports a conservative approach toward the application of accounting principles and estimates.
- Management discloses all financial, budgetary, and programmatic information needed to fully understand the operations and financial condition of the organization.
- Management avoids focus on short-term reported results only.
- Personnel do not submit inappropriate or inaccurate reports in order to meet targets.
- Facts are not exaggerated and budgetary estimates are not stretched to a point of unreasonableness.

d. Organizational Structure

(1) The organizational structure should be appropriate for its size and the nature of its operations. Consider the following:

- The organizational structure facilitates the flow of information throughout the structure.
- The organizational structure is appropriately centralized or decentralized, given the nature of its operations, and management has clearly articulated the considerations and factors taken into account in balancing the degree of centralization versus decentralization.

(2) Key areas of authority and responsibility should be defined and communicated throughout the organization. Consider the following:

- Executives in charge of major activities or functions are fully aware of their duties and responsibilities.

- An accurate and updated organizational chart showing key areas of responsibility is provided to all employees.
- Executives and key managers understand their internal control responsibilities and ensure that their staffalso understand their own responsibilities.

(3) Appropriate and clear internal reporting relationships should be established. Consider the following:

- Reporting relationships have been established and effectively provide managers information they need to carry out their responsibilities and perform their jobs.
- Employees are aware of the established reporting relationships.
- Mid-level managers can easily communicate with senior operating executives.

(4) Management should periodically evaluate the organizational structure and make changes as necessary in response to changing conditions.

(5) The agency should have the appropriate number of employees, particularly in managerial positions. Consider the following:

- Managers and supervisors have time to carry out their duties and responsibilities.
- Employees do not have to work excessive overtime or outside the ordinary workweek to complete assigned tasks.
- Managers and supervisors are not fulfilling the roles of more than one employee.

e. Assignment of Authority and Responsibility

(1) The organization should appropriately assign authority and delegate responsibility to the proper personnel to deal with organizational goals and objectives. Consider the following:

- Authority and responsibility are clearly assigned throughout the organization and this is clearly communicated to all employees.
- Responsibility for decision making is clearly linked to the assignment of authority, and individuals are held accountable accordingly.
- Management has effective procedures to monitor results.

(2) Each employee should know how his actions interrelate with others, taking into account the way in which authority and responsibilities are assigned, and should be aware of the related duties concerning internal control. Consider the following:

- Job descriptions clearly indicate the degree of authority and accountability delegated to each position and the responsibilities assigned.
- Job descriptions and performance evaluations contain specific references to internal control-related duties, responsibilities, and accountability.

(3) The delegation of authority should be appropriate in relation to the assignment of responsibility. Consider the following:

- Employees at the appropriate levels are empowered to correct problems or implement improvements.

- There is an appropriate balance between the delegation of authority at lower levels to get the job done and the involvement of senior-level personnel.

f. Human Resource Policies and Practices

(1) Policies and procedures should be in place for hiring, orienting, training, evaluating, counseling, promoting, compensating, disciplining, and terminating employees. Consider the following:

- Management communicates information to recruiters about the type of competencies needed for the work or participates in the hiring process.
- The agency has standards or criteria for hiring qualified people, with emphasis on education, experience, accomplishment, and ethical behavior.
- Position descriptions and qualifications are in accordance with the standards accepted throughout the MoD of Ukraine for similar jobs.
- A training program has been established and includes orientation programs for new employees and ongoing training for all employees.
- Promotion, compensation, and rotation of employees are based on periodic performance appraisals.
- The importance of integrity and ethical values is reflected in performance appraisal criteria.
- Employees are provided with appropriate feedback and counseling on their job performance and suggestions for improvements.

- Disciplinary or remedial action is taken in response to violations of policies or ethical standards.

- Employment is terminated when deemed necessary, following established policies and laws of Ukraine.

(2) Background checks should be conducted on candidates for employment. Consider the following:

- Candidates who change jobs often are given particularly close attention.

- Hiring standards require investigation to determine if potential employees have criminal records

- References and previous employers are contacted.

- Educational and professional certifications are confirmed.

g. Oversight Groups

(1) Within the organization, there should be mechanisms in place to monitor and review operations and programs. Consider the following:

- Commander has created a temporary or permanent investigative/reviewing unit (financial integrity unit) which is responsible for reviewing the organization’s activities and systems and providing information, analyses, appraisals, recommendations, and counsel to management. The unit includes senior management and professionally trained or experienced staff in financial control systems

(2) The organization should work closely with oversight organizations. Consider the following:

- The organization has a good working relationship with auditors from the Control and Oversight Department of the MoD, and major officials from other MoD oversight agencies.

- High-level organization personnel maintain good working relationships with other executive branch agencies that exercise multi-agency control responsibilities, such as the state tax administration, treasury, and main control and revision office of the Ukraine.

2. Risk Assessment

A precondition to risk assessment is the establishment of clear, consistent organizational goals and objectives at both the entity level and at the activity (program or mission) level. Once the objectives have been set, the organization needs to identify the risks that could impede the efficient and effective achievement of those objectives.

a. Establishment of Entity-Wide Objectives

(1) The organization should establish entity-wide objectives that provide sufficiently broad statements and guidance about what the organization is supposed to achieve, yet are specific enough to relate directly to the organization. Consider the following:

- Management has established overall entity-wide objectives in the form of mission, goals, and objectives.
- The entity-wide objectives relate to and stem from program requirements established by legislation.
- The entity-wide objectives are specific enough to clearly apply to the exact organization instead of applying to all military units/organizations.

(2) Entity-wide objectives should be clearly communicated to all employees, and management obtains feedback signifying that the communication has been effective.

(3) There should be a relationship and consistency between the MoD operational strategies and the organization’s objectives and plans. Consider the following:

- The organization’s objectives support the MoD’s strategic plans.
- The organization’s plans address resource allocations and priorities.
- The organization’s plans and budgets are designed with an appropriate level of detail for various management levels.
- Assumptions made in the organization’s plans and budgets are consistent with the historical experience and current circumstances.

b. Establishment of Activity-Level Objectives

(1) Activity-level (program or mission-level) objectives should flow from and should be linked with an organization’s entity-wide objectives and plans. Consider the following:

- All significant activities are adequately linked to the entity-wide objectives and plans.
- Activity-level objectives are reviewed periodically to ensure continued relevance.

(2) Activity-level objectives should be complementary, reinforce each other, and should not be contradictory.

(3) Activity-level objectives should be relevant to all significant organization processes. Consider the following:

- Objectives have been established for all the key operational activities and the support activities.

- Activity-level objectives are consistent with effective past practices and performance and are consistent with any industry or business norms that may be applicable to the organization's operations.

(4) Activity-level objectives should include measurement criteria.

(5) The organization's resources should be adequate relative to its activity-level objectives. Consider the following:

- The resources needed to meet the objectives have been identified.

- If adequate resources are not available, management has plans to acquire them.

(6) Management should identify those activity-level objectives that are critical to the success of the overall entity-wide objectives. Consider the following:

- Management has identified the processes and activities that must occur if the entity-wide objectives are to be met.

- The critical activity-level objectives receive particular attention and review from management and their performance is monitored regularly.

(7) All levels of management should be involved in establishing the activity-level objectives and should be committed to their achievement.

c. Risk Identification

(1) Management should comprehensively identify risk using various methodologies as appropriate. Consider the following:

- Qualitative and quantitative methods are used to identify risk and determine relative risk rankings on a scheduled and periodic basis.
- How risk is to be identified, ranked, analyzed, and mitigated is communicated to appropriate staff.
- Risk identification and discussion occur in senior-level management conferences.
- Risk identification takes place as a part of short- and long-term forecasting and planning.
- Risk identification occurs as a result of consideration of findings from audits, evaluations, and other assessments.
- Risks that are identified at the employee and mid-management level are brought to the attention of senior-level managers.

(2) Adequate mechanisms should exist to identify risks to the organization arising from external factors. Consider the following:

- Risks posed by new legislation or regulations are identified.
- Risks to the agency as a result of possible natural catastrophes or criminal or terrorist actions are taken into account.
- Identification of risks resulting from the political and economic changes is determined.
- Consideration is given to the risks associated with major suppliers and contractors.
- The organization carefully considers any risks resulting from its interactions with various other governmental entities and parties outside the government.

(3) Adequate mechanisms should exist to identify risks to the organization arising from internal factors. Consider the following:

- Risks resulting from downsizing of organization operations and personnel because of reformation/reorganizing are considered.
- The organization identifies risks associated with business process reengineering or redesign of operating processes.
- Consideration is given to possible risks resulting from the lack of qualifications of personnel hired or the extent to which they have been trained or not trained.
- Risks resulting from heavy reliance on contractors or other related parties to perform critical operations are identified.
- Risk identification activities consider certain human-capital-related risks, such as the inability to provide succession planning and retain key personnel who can affect the ability of the organization or program activity to function effectively and the inadequacy of compensation and benefit programs to keep the organization competitive with the private sector for labor.
- Risks related to the availability of future funding for new programs or the continuation of current programs is assessed.

(4) In identifying risk, management should assess other factors that may contribute to or increase the risk to which the organization is exposed. Consider the following:

- Management considers any risks related to past failures to meet the organization's missions, goals, or objectives or failures to meet budget limitations.

- Consideration is given to risks indicated by a history of improper program expenditures, violations of funds control, or other statutory noncompliance.

(5) Management should identify risks entity-wide and for each significant activity level of the agency.

d. Risk Analysis

(1) After the risks to the agency have been identified, management should undertake a thorough and complete analysis of their possible effect. Consider the following:

- Management has established a formal process to analyze risks, and that process may include informal analysis based on day-to-day management activities.
- Criteria have been established for determining low, medium, and high risks.
- Appropriate levels of management and employees are involved in the risk analysis.
- The risks identified and analyzed are relevant to the corresponding activity objective.
- Risk analysis includes estimating the risk's significance.
- Risk analysis includes estimating the likelihood and frequency of occurrence of each risk and determining whether it falls into the low-, medium-, or high-risk category.
- A determination is made on how best to manage or mitigate the risk and what specific actions should be taken.

(2) Management should develop an approach for risk management and control based on how much risk can be prudently accepted. Consider the following:

- The approach can vary from one organization to another depending upon variances in risks and how much risk can be tolerated.
- The approach is designed to keep risks within levels judged to be appropriate and management takes responsibility for setting the tolerable risk level.
- Specific control activities are decided upon to manage or mitigate specific risks entity-wide and at each activity level. Also, control activity implementation is monitored.

3. Control Activities

Internal control activities are the policies, procedures, techniques, and mechanisms that help ensure that management's directives to mitigate risks identified during the risk assessment process are carried out. Given the wide variety of control activities that organizations may employ, it would be impossible for this tool to address them all. Therefore, the following will address common categories of control activities.

a. Common Categories of Control Activities

(1) *Management Reviews at the Functional or Activity Level.* Organization managers should review actual performance against targets. Consider the following:

- Managers at all activity levels review performance reports, analyze trends, and measure results against targets.
- Both financial and program managers' review and compare financial, budgetary, and operational performance in relation to planned or expected results.

- Appropriate control activities are employed, such as reconciliations of summary information to supporting detail and checking the accuracy of summarizations of operations.

(2) *Management of Human Capital*. The agency should effectively manage the organization's workforce to achieve results. Consider the following:

- The organization has defined the type of leaders it wants through written descriptions of roles, responsibilities, attributes, and competencies and has established broad performance expectations for them.
- Senior leaders and managers attempt to build teamwork, reinforce the shared vision of the organization, and encourage feedback from employees, as evidenced by actions taken to communicate this to all employees and the existence of opportunities for management to obtain feedback.
- Employees are provided orientation, training, and tools to perform their duties and responsibilities, improve performance, enhance their capabilities, and meet the demands of changing organizational needs.
- The compensation system is adequate to acquire, motivate, and retain personnel, and incentives and rewards are provided to encourage personnel to perform at maximum capability.

(3) *Information Processing*. The organization should employ a variety of control activities suited to information processing systems to ensure accuracy and completeness. Consider the following:

- Access to data, files, and programs is appropriately controlled.

(4) *Physical Control Over Vulnerable Assets.* The organization should employ physical control to secure and safeguard vulnerable assets. Consider the following:

- Physical safeguarding policies and procedures have been developed, implemented, and communicated to all employees.
- Assets that are particularly vulnerable to loss, theft, damage, or unauthorized use, such as cash, securities, supplies, inventories, and equipment, are physically secured and access to them is controlled.
- Assets such as cash, securities, supplies, inventories, and equipment are periodically counted and compared to control records; exceptions are examined.
- Cash and negotiable securities are maintained under lock and key and access to them is strictly controlled.
- Forms such as blank checks and purchase orders are sequentially pre-numbered and physically secured with access to them strictly controlled.
- Equipment vulnerable to theft is securely fastened or protected.
- Identification plates and numbers are affixed to office furniture and fixtures, equipment, and other portable assets.
- Inventories, supplies, and finished items and goods are stored in physically secured areas and protected from damage.

- Facilities are protected from fire by fire alarms and sprinkler systems.
- Access to premises and facilities is controlled by fences, guards, or other physical controls.
- Access to facilities is restricted and controlled during nonworking hours.

(5) *Segregation of Duties*. Key duties and responsibilities should be divided or segregated among different people to reduce the risk of error, waste, or fraud. Consider the following:

- No one individual is allowed to control all key aspects of a transaction or event.
- Responsibilities and duties involving transactions and events are separated among different employees with respect to authorization, approval, processing and recording, making payments or receiving funds, review and auditing, and the custodial functions and handling of related assets.
- Duties are assigned systematically to a number of individuals to ensure that effective checks and balances exist.
- Where feasible, no one individual is allowed to work alone with cash, negotiable securities, or other highly vulnerable assets.
- The responsibility for opening mail is assigned to individuals who have no responsibilities for or access to files or documents pertaining to accounts receivable or cash accounts.

- Bank accounts are reconciled by employees who have no responsibilities for cash receipts, disbursements, or custody.
- Management is aware that collusion can reduce or destroy the control effectiveness of segregation of duties and, therefore, is especially alert for it and attempts to reduce the opportunities for it to occur.

(6) *Execution of Transactions and Events*. Transactions and other significant events should be authorized and performed by the appropriate personnel. Consider the following:

- Controls ensure that only valid transactions and other events are initiated or entered into, in accordance with management's decisions and directives.
- Controls are established to ensure that all transactions and other significant events that are entered into are authorized and executed only by employees acting within the scope of their authority.
- Authorizations are clearly communicated to managers and employees and include the specific conditions and terms under which authorizations are to be made.
- The terms of authorizations are in accordance with directives and within limitations established by law, regulation, and management.

(7) *Recording of Transactions and Events.* Transactions and other significant events should be properly classified and promptly recorded. Consider the following:

- Transactions and events are appropriately classified and promptly recorded so that they maintain their relevance, value, and usefulness to management in controlling operations and making decisions.

- Proper classification and recording take place throughout the entire life cycle of each transaction or event, including authorization, initiation, processing, and final classification in summary records.

- Proper classification of transactions and events includes appropriate organization and format of information on original documents (hardcopy paper or electronic) and summary records from which reports and statements are prepared.

(8) *Access Restrictions to and Accountability for Resources and Records.* Access to resources and records should be limited, and accountability for their custody should be assigned. Consider the following:

- The risk of unauthorized use or loss is controlled by restricting access to resources and records to authorized personnel only.

- Accountability for resources and records custody and use is assigned to specific individuals.

- Access restrictions and accountability assignments for custody are periodically reviewed and maintained.

- Periodic comparison of resources with the recorded accountability is made to determine if the two agree, and differences are examined.

- How frequently actual resources are compared to records and the degree of access restrictions are functions of the vulnerability of the resource to the risk of errors, fraud, waste, misuse, theft, or unauthorized alteration.

- Management considers such factors as asset value, portability, and exchangeability when determining the appropriate degree of access restrictions.
- As a part of assigning and maintaining accountability for resources and records, management informs and communicates those responsibilities to specific individuals within the agency and assures that those people are aware of their duties for appropriate custody and use of those resources.

(9) *Documentation*. Internal Control and all transactions and other significant events should be clearly documented. Consider the following:

- The documentation is readily available for examination.
- Documentation for internal control includes documentation describing and covering automated-information systems, data collection and handling, and the specifics of general and application control related to such systems.
- Documentation of transactions and other significant events is complete and accurate. Facilitates tracing the transaction or event and related information from authorization and initiation through processing is completed.
- Documentation, whether in paper or electronic form, is useful to managers in controlling their operations and to any others involved in evaluating or analyzing operations.
- All documentation and records are properly managed, maintained, and periodically updated.

4. Information and Communications

For an organization to run and control its operations, it must have relevant, reliable information, both financial and nonfinancial, relating to external as well as internal events. The organization should also have appropriate channels of communication.

a. Information

(1) Information from internal and external sources should be obtained and provided to management as a part of the organization’s reporting on operational performance relative to established objectives.

(2) Pertinent information should be identified, captured, and distributed to the right people in sufficient detail, in the right form, and at the appropriate time to enable them to carry out their duties and responsibilities efficiently and effectively. Consider the following:

- Managers receive analytical information that helps them identify specific actions that need to be taken.
- Information is provided at the right level of detail for different levels of management.
- Program managers receive both operational and financial information to help them determine whether they are meeting the strategic and annual performance plans and meeting the organization’s goals for accountability of resources.
- Operational information is provided to managers so that they may determine whether their programs comply with applicable laws and regulations.
- The appropriate financial and budgetary information is provided for both internal and external financial reporting.

b. Communications

(1) Management should ensure that effective internal communications occur. Consider the following:

- Top management provides a clear message throughout the organization that internal control responsibilities are important and must be taken seriously.
- Employees' specific duties are clearly communicated to them, and they understand the relevant aspects of internal control, how their role fits into it, and how their work relates to the work of others.
- Acceptable behavior versus unacceptable behavior and the consequences of improper conduct are clearly communicated to all employees.
- Personnel have a means of communicating information upstream within the organization through someone other than a direct supervisor, and there is a genuine willingness to listen on the part of management.
- Mechanisms exist to allow the easy flow of information down, across, and up the organization, and easy communications exist between functional activities, such as between procurement activities and production activities.
- Employees indicate that informal or separate lines of communications exist, which serve as a fail-safe control for normal communications avenues.
- Personnel understand that there will be no reprisals for reporting adverse information, improper conduct, or circumvention of internal control activities.

- Mechanisms are in place for employees to recommend improvements in operations, and management acknowledges good employee suggestions with cash awards or other meaningful recognition.
- Management communicates frequently with internal oversight groups, such as senior management councils, and keeps them informed of performance, risks, major initiatives, and any other significant events.

(2) Management should ensure that effective external communications occur with groups that can have a serious impact on programs, projects, operations, and other activities, including budgeting and financing. Consider the following:

- Open and effective communications channels have been established with customers, suppliers, contractors, consultants, and other groups that can provide significant input on quality and design of the organization's products and services.
- All outside parties dealing with the organization are clearly informed of the organization's ethical standards and understand that improper actions, such as improper billings, kickbacks, or other improper payments, will not be tolerated.
- Communications from external parties, such as other governmental agencies, local governments, and other related third parties, are encouraged since those communications can be a source of information on how well internal control is functioning.

- Management makes certain that the advice and recommendations of auditors and evaluators are fully considered and that actions are implemented to correct any problems or weaknesses they identify.

c. Forms and Means of Communications

(1) The organization should employ various forms and means of communicating important information with employees and others. Consider the following:

- Management uses effective communications methods, which may include policy and procedures manuals, management directives, memoranda, bulletin-board notices, internet and intranet web pages, videotaped messages, e-mail, and speeches.
- Two of the most powerful forms of communications used by management are the positive actions it takes in dealing with personnel throughout the organization and its demonstrated support of internal control.

(2) The organization should manage, develop, and revise its information systems in an effort to continually improve the usefulness and reliability of its communication of information. Consider the following:

- Management continually monitors the quality of information captured, maintained, and communicated as measured by such factors as appropriateness of content, timeliness, accuracy, and accessibility.

5. Monitoring

Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

a. Ongoing Monitoring

(1) Management should have a strategy to ensure that ongoing monitoring is effective and will trigger separate evaluations where problems are identified. Consider the following:

- Management’s strategy provides for routine feedback and monitoring of performance and control objectives.
- The monitoring strategy includes methods emphasizing to program and operational mangers that they have responsibility for internal control and that they should monitor the effectiveness of control activities as a part of their regular duties.
- The monitoring strategy includes identification of critical operational and mission support systems that need special review and evaluation.
- The strategy includes a plan for periodic evaluation of control activities for critical operational and mission support systems.

(2) In the process of carrying out their regular activities, organization personnel should obtain information about whether internal control is functioning properly. Consider the following:

- Operating reports are integrated or reconciled with financial and budgetary reporting system data and are used to manage operations on an ongoing basis. Management is aware of inaccuracies or exceptions that could indicate internal control problems.
- Operating management compares production or other operating information obtained in the course of its daily

activities to system-generated information and follows up on any inaccuracies or other problems that might be found.

- Operating personnel are required to sign off on the accuracy of their unit's financial statements and are held accountable if errors are discovered.

(3) Communications from external parties should corroborate internally-generated data or indicate problems with internal control. Consider the following:

- Management recognizes that customer payment for invoices help to corroborate billing data, while customer complaints indicate that deficiencies may exist; and these deficiencies are then investigated to determine the underlying causes.
- Communications from vendors and monthly statements of accounts payable are used as control-monitoring techniques.
- Supplier complaints about any unfair practices by organization purchasing agents are investigated.
- Control activities that should have prevented or detected any problems that arose, but did not function properly, are reassessed.

(4) Data recorded by information and financial systems should be periodically compared with physical assets, and discrepancies should be examined. Consider the following:

- Inventory levels of materials, supplies, and other assets are checked regularly; differences between recorded and actual amounts are corrected; and the reasons for the discrepancies are resolved.

- The frequency of the comparison should be a function of the vulnerability of the asset.

- Custodial accountability for assets and resources is assigned to responsible individuals.

(5) Meetings with employees should be used to provide management with feedback on whether or not internal control is effective. Consider the following:

- Relevant issues, information, and feedback concerning internal control that arose at training seminars, planning sessions, and other meetings are captured and used by management to address problems or strengthen the internal control structure.

- Employee suggestions on internal control are considered and acted upon as appropriate.

- Management encourages employees to identify internal control weaknesses and report them to the next supervisory level.

(6) Employees should regularly be asked to state explicitly whether they comply with the organization’s code of conduct. Consider the following:

- Personnel periodically acknowledge compliance with the code of conduct.

- Signatures are required to document performance of critical internal control functions, such as reconciliations.

b. Separate Evaluations

(1) The scope and frequency of separate evaluations of internal control should be appropriate for the organization. Consider the following:

- Consideration is given to the risk assessment results and the effectiveness of ongoing monitoring when determining the scope and frequency of separate evaluations.
- Separate evaluations are often prompted by events such as major changes in management plans or strategies, major expansion or downsizing, significant changes in operations or processing of financial or budgetary information, or by decision of the oversight MoD agencies.
- Separate evaluations usually are conducted by external auditors, but can be conducted by personnel with the required skills from the evaluated organization.

(2) The methodology for evaluating the organization's internal control should be logical and appropriate. Consider the following:

- The methodology used may include self-assessments using checklists, questionnaires, or other such tools.
- The separate evaluations may include a review of the control design and direct testing of the internal control activities.
- In organizations where large amounts of data are processed by the information and financial systems, separate evaluation methodology employs computer-assisted audit techniques to identify indicators of inefficiencies, waste, or abuse.
- The evaluation team develops a plan for the evaluation process to ensure a coordinated effort.
- If the evaluation process is conducted by the organization's employees, it is managed by an executive with the requisite authority, capability, and experience.

- The evaluation team gains a sufficient understanding of the organization’s missions, goals, and objectives and its operations and activities.
- The evaluation team analyzes the results of the evaluation against established criteria.
- The evaluation process is properly documented.

(3) Deficiencies found during separate evaluations should be promptly resolved. Consider the following:

- Deficiencies are promptly communicated to the individual responsible for the function and also to at least one level of management above that individual.
- Serious deficiencies and internal control problems are promptly reported to top management.

c. Audit Resolution

(1) The organization should have a mechanism to ensure the prompt resolution of findings from Control and Oversight Department audits and other reviews. Consider the following:

- Management determines the proper actions to take in response to findings and recommendations.
- Corrective action is taken or improvements made within established time frames to resolve the matters brought to management’s attention.
- Management considers consultations with auditors and reviewers when they are believed to be helpful in the audit resolution process.

(2) Organizational management should be responsive to the findings and recommendations of audits and other reviews aimed at strengthening internal control. Consider the following:

- Executives with the proper authority evaluate the findings and recommendations and decide upon the appropriate actions to take to correct or improve control.
- There is follow-up on desired internal control actions to verify implementation.

(3) The organization should take appropriate follow-up actions with regard to findings and recommendations of audits and other reviews. Consider the following:

- Problems with particular transactions or events are corrected promptly.
- The underlying causes giving rise to the findings or recommendations are investigated by management.
- Actions are decided upon to correct the situation or take advantage of the opportunity for improvements.
- Management and auditors follow up on audit and review findings, recommendations, and the actions decided upon to ensure that those actions are taken.
- Top management is kept informed through periodic reports on the status of audit and review resolution so that it can ensure the quality and timeliness of individual resolution decisions.

E. PROCUREMENT FRAUD DICTIONARY

A procurement fraud dictionary is an effective tool. However, it does not include all possible fraud schemes and must be updated continuously. This dictionary is based on materials from the following websites: U.S. Department of Defense Office of the Inspector General (http://www.dodig.mil/Inspections/APO/fraud/) and the U.S. Department of Justice National Procurement Fraud Task Force (http://www.usdoj.gov/criminal/npftf).

1. Rigged Specifications

Scheme: The requesting organization, in developing specifications, tailors them to meet the qualifications of one particular company, supplier, or product. This applies mostly to procurement of special equipment and fixtures. Military unit's managers involved in such a scheme could be seeking bribes or illegal gratuities.

Detection: Compare specifications established for a particular procurement with the contractor's description of its product or service. Nearly identical matches would indicate the possibility of rigged specifications.

Other indicators of rigged specifications include receipt of only one bid, one bid significantly lower than others, and sole source procurement.

2. Collusive Bidding

Scheme: A group of companies with the capability of providing the same goods or services conspire to exchange bid information on contract solicitations and to take turns at submitting the low bid. Such action may be carried out in collusion with procuring managers and also involve bribery or illegal gratuities.

Detection: Examine contract solicitation files for a small number of companies doing similar work on what appears to be a rotating basis. Fairly wide disparity between winning and losing bids, unsuccessful bidders who become subcontractors after contract award, and bids that are very close on nonstandard items with no suggested retail price should be investigated. Be suspicious of possible fraudulent activity if competing contractors regularly socialize or contractors and military unit's procurement personnel socialize.

3. Failure to Meet Specifications

Scheme: A contractor, in order to increase profits, provides goods or services that do not comply with contract specifications in quantity or quality. For example, a contractor uses one coat of paint rather than two or pours six inches of aggregate on road surfaces instead of nine. Qualitative noncompliance with contract specifications includes using inferior or substitute materials.

Detection: Obtain and review inspection reports to determine whether the work performed and materials used in a project were inspected and considered acceptable. A lack of inspection indicates potential problems in meeting contract specifications.

4. False Invoices

Scheme: Where contracts provide for the continual supply of merchandise over a period of time, invoices may be inflated or submitted for goods not delivered. This situation is particularly applicable to open-ended purchase agreements.

Detection: Account for purchases through comparison of physical inventory with inventory purchases recorded in the organization’s accounting records.

5. Duplicate Contract Payments

Scheme: The contractor submits copies of the same invoice for payment or submits more than one original invoice for the same goods or services (most often small purchases). This tactic may be accomplished through collusion between the contractor and the requesting military unit’s manager.

Detection: Review payment documents for a specific time period, checking for same payee, amounts paid, and items purchased. Be especially alert to payments supported by photocopies of invoices rather than originals. Unusually large quantities of a single item purchased over a short period of time may indicate the possibility of duplicate payments.

6. Change Orders Abuse

Scheme: A company bidding on a contract, in collusion with personnel from the requesting organization, submits a low bid to ensure receiving the contract award. However, the company has been assured that change orders will be issued during the life of the contract to more than compensate for the low bid. After the contract is awarded, the contractor and the military unit responsible official share the excessive reimbursements.

Detection: Analyze contract change orders for the addition of new items and for significant increases in scope, quantities, and price of existing contract items.

7. Excessive Small Purchases of Tools, Supplies, etc.

Scheme: Items are purchased and subsequently diverted for personal use. This includes items which are not required or quantities purchased in excess of requirements.

Detection: Obtain a listing of small purchases made over a specified period of time and rearrange the list by name of purchaser and organizational unit.

8. Split Purchases

Scheme: Procurement is split into two or more purchase orders to avoid the scrutiny required for larger-dollar-value contracts. Splitting the requirement may waste funds by losing the economic advantage of volume purchasing. Favoritism or other forms of fraud are easier to conceal when small purchase methods are used.

Detection: Scrutinize invoices and supporting documentation for evidence. Look for identical items that were purchased in different quantities simultaneously or within a short period of time. Also, the project could be split by the type of work (material and labor for the same project paid separately).

9. Phantom Contractors

Scheme: An invoice(s) from a nonexistent company is submitted for payment. This fraud could be perpetrated by accounting personnel or someone responsible for administration of the project.

Detection: Scrutinize invoices and supporting documentation. Look for oddly-named vendors and strange addresses or telephone numbers. Be alert to payments supported by photocopies of invoices.

10. Commingling of Contracts

Scheme: A company is awarded separate contracts for various efforts, e.g., electrical contracts, painting contracts, flooring contracts, etc. Each contract allows charges for services or items used in the other contracts as well. Through collusion, the contractor can bill for the same work or supplies on each of the contracts. A similar scheme involves mixing of inventories to prevent identification of purchase with special funds. For example, paint purchased for government-owned quarters may be used for painting an individual's home. Items purchased with office supply funds may be used for a worker's personal use..

11. Abnormal Increase in Consumption of Fuel or Automotive-Supply Items

Scheme 1: Abnormally high consumption of fuel or common supply items such as automotive parts, tools, and individual equipment indicates the items could have been diverted for personal use or resale.

Scheme 2: Maintenance personnel may charge unnecessary parts to vehicle maintenance and divert these parts for personal use or gain. For example, vehicle maintenance records identify fourteen tire replacements in 8,148 miles, five new batteries in 100 miles, and seven tune-ups in 8,000 miles.

Scheme 3: Government funds are used for replacement parts in new vehicles. If vehicle records show that parts procured with government funds are being used in new vehicles, there is a possibility that the parts are being sold for personal gain.

12. Overstatement of Shipment Weights

Suppliers may be defrauding the military unit by artificially inflating the weight of a shipment. They could use the following methods to "bump" or increase the true weight of a shipment:

- Body bumping: A lightweight driver sits in the van when getting the tare weight and a heavier driver gets the gross weight of the van.
- Fuel Bumping: Getting the tare weight with less than a full tank of gas and the gross weight with a full tank.
- Packing/Equipment Bumping: Getting the tare weight without the required packing and equipment (blankets, ladders, snow chains, etc.) and getting the gross weight with the equipment included could result in a net increase of several hundred pounds.

13. Large Year-End Purchases for Nonspecific Items

Employees may obligate all year-end funds to a local vendor to establish a credit balance account. Future purchases are then made against this account.

F. SUMMARY OF GUIDELINES

FRAUD INDICATOR GUIDELINES

Program component	Activities
Fraud Detection	Detect if fraud is possible by evaluating different indicators: situational, accounting related, documentary, and behavioral.
Follow-up Detection	If a fraud investigative unit identifies a "red flag" event, it

Procedures	should extend auditing procedures and immediately inform the Control and Oversight Department of MoD.
Fraud Resolution	If fraud is identified, certain actions must be taken by commander. These include criminal referral to fraudsters, disciplinary, and civil actions as well as internal control remediation.

Table 4. Fraud Indicator Guidelines

GUIDELINES FOR A BASIC ANTI-FRAUD PROGRAM

Basic Fraud Prevention Program	• Create a fraud task force • Establish whistle-blower program • Institute an anti-fraud hotline • Design and deliver a fraud awareness training program.

Table 5. Guidelines for a Basic Anti-fraud Program

GUIDELINES FOR ESTABLISHING AN ADVANCED ANTI-FRAUD INTERNAL CONTROL PROGRAM

The Control Environment	• Establish appropriate “tone at the top,” atmosphere of integrity, and ethical values • Develop a policy and a methodology to investigate potential occurrences of fraud • Develop an appropriate management philosophy and operating style • Correct organizational structure to achieve transparency and effective internal control • Assign proper authority and responsibility
Risk Assessment	• Establish entity-wide and activity-level objectives • Identify risks and conduct analysis

	• Involve appropriate personnel in the risk assessment process
Control Activities	• Conduct regular reviews at the functional or activity level • Establish physical control over valuable and sensitive assets • Have a proper segregation of duties • Ensure the proper authorization of significant transactions and events
Information and Communications	• Establish proper channels of communication • Establish policies for reporting of fraudulent activity
Monitoring	• Provide a periodic internal evaluation of anti-fraud controls. • Use independent evaluations of fraud prevention programs by Control and Oversight Department of MoD.

Table 6. Guidelines for Establishing an Advanced Anti-fraud Internal Control Program

VI. SUMMARY, CONCLUSION, AND RECOMMENDATIONS

A. SUMMARY

The primary purpose of this project was to review the best practices of American organizations in the areas of internal control and fraud prevention and to provide guidelines for fraud detection and fraud deterrence for commanders. The *Commander's (Executive Officer's) Guide for Detecting and Deterring Procurement Fraud in a Military Unit (or Organization) of the Armed Forces of Ukraine* incorporates several tools from fraud prevention documents such as the Office of Management and Budget's Circular A-123 of 1981, the Federal Managers' Financial Integrity Act of 1982 (FMFIA), COSO's *Internal Control—Integrated Framework*, the GAO's "Standards for Internal Control in the Federal Government," and others. This research found that entities can take several actions to prevent fraud by evaluating indicators of fraudulent activity, establishing and developing anti-fraud processes and controls, and creating a culture of honesty and high ethical behavior.

Organizationally, this MBA project is comprised of six chapters. Chapter I provided an introduction, outlining the background, purpose of the project, research objectives and methods, and the organization of this project. Chapter II discussed internal control and fraud management found in the literature review. Chapter III identified the Ukrainian Armed Forces as a unique and dynamic control environment in the process of transformation. Chapter IV explored the complex, interrelated mix of managerial issues that will confront the Ukrainian military as its internal control system undergoes change, such as organizational culture, leadership, and execution challenges. Finally, Chapter V provided guidelines for fraud detection and fraud deterrence and for internal control to assist commanders in establishing a wide-range effective internal control system.

The research methodology used for this project consisted of collecting relevant data from a variety of sources for analysis. Books, instructions, internet sites, and journal articles were reviewed to create a comprehensive outline of the methods, policies, and practices used in the United States to fight fraud.

B. CONCLUSION

The situation in the Ukrainian Armed Forces, as well as throughout the Ukraine, demands that an appropriate and effective internal control system be put in place. The Ukrainian government has approved a long-term strategy to create an internal control system based on COSO standards. A sound internal control system will effectively uphold the corporate vision, communicate strategies throughout the organization, and link these strategies with the objectives at all levels. The objectives of an effective internal control system should do more than merely protect an organization from fraud. COSO's landmark report on internal control suggests three main goals: efficiency and effectiveness of operations, accuracy of financial reporting, and compliance with laws and regulations.

Governmental internal control, as a system, must be built on laws and legislation. Currently Ukraine is lacking such legislation. Incorporating and implementing an American-style internal control system, while also considering the characteristics and philosophy of the Ukrainian armed forces, will be a challenging task.

Not only is the implementation of an internal control system a requirement of Ukrainian law, but it is also a necessary tool for educating managers and other stakeholders. Leaders and key personnel should understand the purpose and vision of internal control. To increase general awareness about internal control issues, simple but highly visible short-term benefits such as those suggested in the *Commander's Guide* are vital. The author believes that the guide will prove to be a useful instrument for commanders in Ukrainian government organizations.

C. RECOMMENDATIONS

The *Commander's Guide has* a limited number of applications--the procurement functions of a military organization. Nevertheless, it suggests several generally applicable measures against fraud, such as hotlines, an analysis of fraud perpetrators' reasons for committing fraud, and the creation of an atmosphere of financial integrity. Follow-on development of this project may include the creation of similar guides for other categories of fraud and the incorporation of anti-fraud programs into a wide-ranging internal control system.

Effective internal control for the Ukrainian Armed Forces remains a major goal. The suggested Commander’s Guide contains guidelines that can be incorporated into an internal control system at the operational or strategic level of the Ukrainian government. Another possibility for using the guide is in testing the applicability of American models to the Ukrainian government. If results of an implementation at the organizational level are positive, it could serve as the basis for a top-level internal control system.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Albrecht, W.S., Romney, M.B., Cherrington, D.J., Payne, I.R., & Roe, A.V. (1982). *How to detect and prevent business fraud*. Englewood Cliffs: Prentice-Hall, Inc.

Albrecht, W.S., Albrecht, C., Albrecht, C.C., (2008) Current Trends in Fraud and its Detection. *Information Security Journal: A Global Perspective, 17:2-12, 2008.*

American Institute of Certified Public Accountants (AICPA). (2002). Statement on Auditing Standards [SAS] No. 99. *Consideration of Fraud in a Financial Statement Audit.*

The Association of Certified Fraud examiners' (ACFE), (2007). *Fraud Examiner's Manual*, 2007

Biegelman, M.T., Bartow, J.T. (2006). *Executive Roadmap to Fraud Prevention And Internal Control*. Hoboken: John Wiley & Sons, Inc.

Broader, J.F., (2000). *Risk Analysis and the Security Survey* (2nd Ed.). Boston: Butterworth-Heinemann.

Cadmus, B., & Child, R. (1953). *Internal Control Against Fraud and Waste*. New York: Prentice-Hall, Inc.

Cabinet of Ministers of Ukraine. (2005). Resolution the Cabinet of Ministers of Ukraine No. 1232, of December 21, 2005.

Choo, F., Tan, K., (2007). An "American Dream" theory of corporate executive Fraud. *Accounting forum,* Vol. 31, issue 2, 2007, pp. 203-215.

Committee of Sponsoring Organizations of the Treadway Commission (COSO), (1992,1994) *Internal Control – Integrated Framework* Retrieved June 8 from http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/InternalControls/COSO/PRDOVR~PC-990009/PC-990009.jsp

Encyclopedia Britannica. (2009). Retrieved April 01, 2009, from http://www.britannica.com/EBchecked/topic/217591/fraud

Goldman, P. (2008). The New Fraud Triangle: Another Dimension in Employee Fraud Motivation, Association of Certified Fraud Examiners, July 2008, *Fraud Examiner Newsletter,* retrieved June 8, 2009 from http://www.acfe.com/newsletters/fraud-examiner.asp?copy=july08-goldmann-column

The Institute of Internal Auditors, the American Institute of Certified Public Accountants, Association of Certified Fraud Examiners. (2008). *Managing the business risk of fraud: A practical guide.* Retrieved June 8, 2009 from http://www.acfe.com/ documents/managing-business-risk.pdf

Internal Control Systems. (2001). Encyclopedia of Business and Finance. Ed. Allison McClintic Marion. Gale Cengage,. eNotes.com. 2006. Retrieved June 8, 2009 from http://www.enotes.com/business-finance-encyclopedia/internal-control-systems

JRS Consulting glossary. (2009). Reprieved June 8, 2009 from http:// www.jrsconsulting.net/freearticles_21.html

Kotter, J.P. (1988). *The Leadership Factor*. New York:The Free Press.

———. (1990). *A Force for Change: How Leadership Differs from Management.* The New York: Free Press.

———. (1996). *Leading change.* Boston: Harvard Business School Press.

———. (1999). *What Leaders Really Do*. Boston: Harvard Business Review Book.

McShane, L.S. (2007) *Organizational behavior [essentials]*. Boston:Mcgraw-Hill Irwin.

Ministry of Defense of Ukraine. (2001). Directive No. 170, May 29, 2001 *Principle of Control And Oversight Service in the Ministry of Defense of Ukraine.*

———.(2002). Directive D-5, May 10, 2002 *About Separation of Responsibility over Financial Control Between Financial Department and Control and Oversight department.*

———. (2008). *White Book 2007 Defense Policy of Ukraine*, Kyiv, Retrieved June 8, 2009 from http://www.mil.gov.ua/files/white_book/ white_book_en2007.pdf

———. (2009). *White Book 2008 Defense Policy of Ukraine*, Kyiv, Retrieved June 8, 2009 from http://www.mil.gov.ua/files/white_book/ wb_2008_en.pdf

Nagel, K. & Company, LLC's d/b/a Sarbanes-Oxley. Retrieved June 8, 2009 from http://www.sarbanes-oxley.com/displaysection.php?level=2&pub_id=IC-Primer&chap_id=IC1&message_id=144

Network-centric Operations Industry Consortium.(2009). Retrieved Juhe 8, 2009 from https://www.ncoic.org/wiki/NCW

Office of Management and Budget Circular No. A-123, *Management's Responsibility for Internal Control*, December 21, 2004, Retrieved June 8, 2009 from http://www.whitehouse.gov/omb/circulars/a123/a123.html

Outlines of Director of Financial Department Ministry of Defense of Ukraine for annual meeting with chief financial officers (2008).

Public Company Accounting Oversight Board (PCAOB) (March 9, 2004). Auditing Standard No. 2*, An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements.* Retrieved June 8, 2009 from http://www.pcaobus.org/Rules/Rules_of_the_Board/Auditing_Standard_2.pdf

Pasmore, W.A. (1988). *Designing Effective Organizations: The Sociotechnical Systems Perspective.* New York, NY: John Wiley and Sons.

President of Ukraine Office. (1995). Decree of President of Ukraine No. 335, April 27, 1995.

———.(2009). Decree of President of Ukraine No. 2/2009, January 10, 2009.

Ramamoorti, S., (2008). The Psychology and Sociology of Fraud: Integrating the Behavioral Sciences Component Into Fraud and Forensic Accounting Curricula. *Issues in Accounting Education, Vol. 23, No. 4, November 2008, pp.521-533*

Russell, S.J.*;* Norvig, P (2003), *Artificial Intelligence: A Modern Approach* (2nd ed.), Upper Saddle River, NJ: Prentice Hall⁄Pearson Education.

Senge, P.M. (1990) *The Fifth Discipline: The Art and Practice of The Leading Organization.* New York, NY: Currency Doubleday.

Ukraine Verhovna Rada. (1993). Law of Ukraine No. 2939-XII, January 26, 1993 *On the Governmental Control and Revision service of Ukraine.*

United State Agency for International Development (USAID). (2009) *Fraud Indicators Handbook*. Retrieved June 8, 2009 from http://www.usaid.gov/oig/hotline/fraud_awareness_handbook_052201.pdf

United States Congress. (2002, July 30) Public Law 107–204, 107th Congress, *Sarbanes-Oxley Act.* Retrieved June 8, 2009 from http://www.sec.gov/about/laws/soa2002.pdf

———. House. Committee on Government Reform. (2005, February 16). *Improving internal controls: A review of changes to OMB Circular A-123*. Hearing before the Subcommittee on Government Management, Finance, and Accountability of the Committee on Government Reform, House of Representatives, 109th Congress, first session. Retrieved June 8, 2009, from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname= 109_house_hearings&docid=f:20879.pdf

United States Department of Defense. (1996, August 26). *Internal Management Control (MC) program*. DoD Directive 5010.38.

———. (1996, August 28). *Management Control (MC) program procedures.* DoD Instruction 5010.40.

———. (2006, January 4). *Managers' Internal Control (MIC) Program Procedures.* DoD Instruction 5010.40.

United States Government Accountability Office. (2001). *Internal control standard: internal control management and evaluation tool*. (GAO Report 01-1008G).

United State Inspector General (2009) *Shell Company and Suspect Purchases,* Retrieved June 8, 2009 from http://www.dodig.mil/Inspections/APO/fraud/scenarios_pdfs/ PurchaseCards.pdf

United States Office of Management and Budget (OMB). (1982). *Financial Managers Financial Integrity Act of 1982.* Retrieved June 8, 2009, from http://www.whitehouse.gov/ omb/financial/fmfia1982.html

Whittington, O., & Pany, K. (2008). *Principles of auditing and other assurance services* (16th ed.). New York: McGraw Hill.

ENDNOTES15

1 Actual amount is UAH 2.96 million

2 Actual amount is UAH 965.9 thousand

3 Any research which is used to answer a specific question, determine why something failed or succeeded, solve a specific, pragmatic problem, or to gain better understanding (JRS Consulting glossary).

4 According to definitions from the interdisciplinary systems theory, it is a system that interacts with an environment (surrounding entities, systems, etc) in opposition to a closed, self-sufficient system. Because fraudulent activity inputs from the environment are crucial and modify behavior (opportunity, motivation), the system must be open.

5 The OMB website (http://www.whitehouse.gov/omb/circulars/) defines circulars as "instructions or information issued by OMB to Federal agencies. These are expected to have a continuing effect of two years or more."

6 FMFIA, an abbreviation for Federal Managers' Financial Integrity Act of 1982, required that each federal agency establish systems of internal administrative controls and accounting in compliance with standards of the comptroller general. It also requires the General Accounting Office (GAO) to issue standards for internal control in government.

7 The last revision of the above-mentioned standards is dated by November 1999. It became widely known throughout the government as the "Green Book." Since 1983 standards were updated because "changes in information technology, emerging issues involving human capital management, and requirements of recent financial management-related legislation have prompted renewed focus on internal control"(GAO-01-1008G, 2001 p.1). Actually the "Green Book" is successful adaptation and simplification for governmental needs theoretical concepts from COSO ICIF.

8 Note that information systems should be the part of a communication system. Communication is a broader concept than just informational exchange. COSO agrees that

all personnel “need to receive a clear message from top management that internal control responsibilities must be taken seriously” or “understand the relevant aspects of the internal control system, how they work and his or her role and responsibility in the system” (ICIF, p.63). However, “understanding” or communication is different from just receiving information. For detailed discussion about communication see, for example, Jim Suchan, “The Effect of Language and Metaphor on Managerial Communication Thinking and Action.”

9 This is a simplification; the real structure is much more complex (Figure 1), including support command, special forces, joint rapid-reaction forces, etc., but these entities are not concerned with issues surrounding centralized financial control.

10 See Preamble section about differences in understanding of internal control.

11 Land forces have three territorial control and oversight directorates down the structure with the same level of responsibility as the service level.

12 This number is subject to regular changes because of structural reformations in the armed forces.

13 Calculated by author from different sources related to the organizational strength of control and oversight services during his service as a chief of general-policy division in the Department of Finance and accurate for 2006–2007.

14 Calculated salary and per diem expenditures only. For conversion of hrivnas in dollars, a rate of 8UAH per 1USD was used.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California